



DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
2 NAVY ANNEX
WASHINGTON, DC 20380-1775

NAVMC DIR 3500.86
C 469
20 JUL 05

NAVMC DIRECTIVE 3500.86

Subj: ANTITERRORISM/CRITICAL INFRASTRUCTURE PROTECTION TRAINING AND
READINESS MANUAL, (SHORT TITLE: AT/CIP T&R MANUAL)

Ref: (a) MCO P3500.72A
(b) MCO 1553.3A
(c) MCRP 3-0A
(d) MCO 1553.2A
(e) MCRP 3-0B
(f) MCO 3500.27A

Encl: (1) Locator Sheet

1. PURPOSE. Per reference (a), this manual establishes training standards, regulations, and policies regarding the training of Marines and assigned Navy personnel performing AT/CIP functions.

2. CANCELLATION. MCO 1510.114.

3. INFORMATION.

a. The training events in this order will be used to standardize unit training throughout the community, focus on Mission Essential Tasks for the community, and establish a framework for assessment of unit and individual training readiness. It includes unit and individual training standards to be used by unit commanders and formal schools for the development of training plans, curricula, and records of training accomplished in order to establish a framework for identifying training achievements, training gaps, and objective assessments of readiness associated with the training of Marines.

b. CG, TECOM will update this T&R Manual as necessary to provide current and relevant training standards to commanders. Commanders will incorporate these training events into their training plans to the extent that the events support their unit's Mission Essential Tasks and to the extent that time and other resources are available.

c. All questions pertaining to the Marine Corps Ground T&R Program and Unit Training Management should be directed to: CG, TECOM (C 469), 3300 Russell Road, Quantico, VA 22134.

4. SCOPE

a. Commanders will review, update, and submit unit Mission Essential Task Lists (METL) per references (b) and (c).

b. Per reference (b), commanders shall conduct an internal assessment of the unit's ability to execute each MET and prepare a definitive plan of

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

NAVMC DIR 3500.86
20 JUL 05

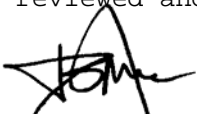
attack to achieve MET proficiency by developing long-, mid-, and short-range training plans to achieve proficiency in each MET.

c. Using this T&R Manual and other pertinent references, commanders will conduct evaluations (informal and formal) of their unit's ability to accomplish their METs. These training evaluations will be conducted at appropriate points in the unit's training cycle to determine MET proficiency and adjust training priorities.

d. Formal school directors and commanders will establish or review programs of instruction per reference (d) to ensure compliance with core individual training requirements as set forth in this Order.

5. COMMAND. This Directive is applicable to the Marine Corps Total Force.

6. CERTIFICATION. This Directive is reviewed and approved this date.



T. S. JONES
By direction

Distribution: PCN 10303370600

Copy to: 7000106 (3)
7000144/70000260/8145001 (2)

RECORD OF CHANGES

Log completed change action as indicated

Change Number	Date of Change	Date Entered	Signature of Person Incorporating Change

TABLE OF CONTENTS

CHAPTER

- 1.....OVERVIEW
- 2.....MISSION ESSENTIAL TASKS
- 3.....COLLECTIVE TRAINING
- 4.....ANTITERRORISM OFFICER INDIVIDUAL TRAINING

APPENDICES

- A.....REFERENCES
- B.....GLOSSARY OF TRAINING & READINESS MANUAL TERMS
- C.....ANTITERRORISM DEFINITIONS
- D.....AT CHECKLIST FOR COMMANDERS AND AT OFFICERS
- E.....SUGGESTED VA METHODOLOGIES
- F.....DOD FPCON SYSTEM (from DoD 5000.12H)
- G.....SAMPLE INSTALLATION ANTITERRORISM PLAN FORMAT (from
MCO 3302.1D)
- H.....TERRORIST INCIDENT RESPONSE MEASURES CHECKLIST
- I.....TERRORIST SURVEILLANCE DETECTION
- J.....AT SECURITY CONSIDERATIONS FOR THE CONTRACTING FORCES
- K.....FAMILY SECURITY QUESTIONS
- L.....HOUSEHOLD SECURITY CHECKLIST
- M.....GROUND TRANSPORTATION SECURITY TIPS
- N.....PERSONAL VEHICLE TIPS AND DRIVING SECURITY CHECKLIST
- O.....AIR TRAVEL SECURITY TIPS
- P.....USE OF PROTECTIVE SECURITY DETAILS
- Q.....SPECIFIC CONSTRUCTION PROTECTIVE MEASURES
- R.....MAIL HANDLING SUSPICIOUS PACKAGES
- S.....ABBREVIATIONS AND ACRONYMS

(This page intentionally left blank)

AT/CIP T&R MANUAL

CHAPTER 1

OVERVIEW

	<u>PARAGRAPH</u>	<u>PAGE</u>
INTRODUCTION	1000	1-3
CORNERSTONE ORDERS	1010	1-3
ORGANIZATION	1020	1-3
T&R EVENT CODING.	1030	1-3
EVALUATION-CODED (E-CODED) EVENTS	1040	1-5
COMBAT READINESS PERCENTAGE (CRP) CALCULATION	1050	1-5
T&R EVENT COMPOSITION	1060	1-6
UNIT TRAINING.	1070	1-8
REQUIREMENTS FOR COLLECTIVE TRAINING	1080	1-8
NUCLEAR, BIOLOGICAL, CHEMICAL (NBC) TRAINING	1090	1-9
NIGHT TRAINING	1100	1-9
APPLICATION OF SIMULATION.	1110	1-9
UNIT TRAINING MANAGEMENT	1120	1-10
EVALUATION OF TRAINING.	1130	1-10
OPERATIONAL RISK MANAGEMENT (ORM)	1140	1-10
BILLETS REQUIRING FORMAL SCHOOL ATTENDANCE	1150	1-11
ACADEMIC TRAINING	1160	1-12
CAREER PROFESSIONAL READING	1170	1-14
CONCLUSION.	1180	1-15

(This page intentionally left blank)

1000. INTRODUCTION

The purpose of the Marine Corps Ground Training and Readiness (T&R) Program is to provide the commander with training standards for all ground personnel. The goal is to develop unit warfighting capabilities, not to measure the proficiency of individuals. The performance standards are designed to ensure proficiency in core competencies. An effective T&R program is the first step in providing a commander with a unit capable of accomplishing any and all of its assigned combat missions. The T&R program provides the fundamental tools for commanders to build and maintain unit combat readiness. Using these tools, training managers can construct and execute an effective training plan that supports the unit's mission essential task list (METL). More detailed information on the Marine Corps Ground T&R Program can be found in reference (a) (MCO P3500.72).

1010. CORNERSTONE ORDERS

Guidance for all training and evaluation in the Marine Corps, from entry-level training at the formal schools to advanced PME for senior enlisted and officers, is found in what are called the Cornerstone Orders. All training and evaluation programs throughout the Marine Corps were designed based on the guidance provided in these orders. The Cornerstone Orders are:

- a. MCO 1553.1B The Marine Corps Education and Training System
- b. MCO 1553.2A Management for Marine Corps Formal Schools and Training Detachments
- c. MCO 1553.3A Unit Training Management
- d. MCO 1553.4A Professional Military Education

1020. ORGANIZATION

T&R Manuals are organized in one of two methods: unit-based or community-based. Unit-based are written to support a type unit (i.e. Infantry, Artillery, Tanks). Community-based are written to support an Occupational Field, a group of like Military Occupational Specialties (MOSs) not assigned to an OccFld, or billets within an organization (i.e., Communications, NBC, Supply Chief). They are comprised of chapters that contain core training standards that list associated unit METs and chapters that contain individual training standards (ITS) for each MOS, billet, etc. This manual follows the community based method even though an Antiterrorism Officer is not an MOS, and is organized in the following manner:

- a. Table of Contents
- b. Mission Essential Task List Matrix
- c. Collective Training Standards
- d. Individual Training Standards
- e. Annexes

1030. T&R EVENT CODING

Antiterrorism T&R events are coded for ease of reference. Each event normally has a 4-4-4 digit identifier. In the first 4 digit set, the first two characters represent the Community (AT), the second two characters represent the associated Mission Essential Task (e.g., Intelligence Support

(IS), Critical Infrastructure Protection (CI), Security Operations (SO), Conduct Antiterrorism Training (TR), and Conduct Antiterrorism Planning (PL)). The code: ATSO, pertains to Antiterrorism Security Operations. The next field consists of 4 characters, the first three characters represent the functional area. The functional areas are: Intel (INT), Critical Infrastructure Protection (CIP), Planning (PLN), Operations (OPS), and Training (TRN). The last character is a number that corresponds to a location and/or type of organization, such as a post or installation, CONUS or OCONUS as follows; Post, Station, and Installation CONUS or OCONUS is (1), Deployed Forces is (2), and both Post, Station, Installation CONUS and OCONUS, and Deployed Forces is (3). For example, the first two fields may look like this, ATSO-TRN3- meaning Antiterrorism Security Operations that pertain to both base station installation CONUS or OCONUS and deployed forces. The last field contains four characters that represent the level and sequence of the event. 1000 level events are individual core skill events and 2000 level events are individual core plus events. 3000 to 8000 level events are collective events accomplished at the unit level. 3000 level events are fire team level events, 4000 is squad level, 5000 is platoon level, 6000 is company level, and 7000 is battalion level. Finally, an 8000 level event would entail a MEF, MARFOR size event. The last three numbers are the sequence numbers used to discriminate the event from all others. The T&R event levels are shown in Figure (1-2). An example of the T&R event coding used in this manual is shown in Figure (1-3).

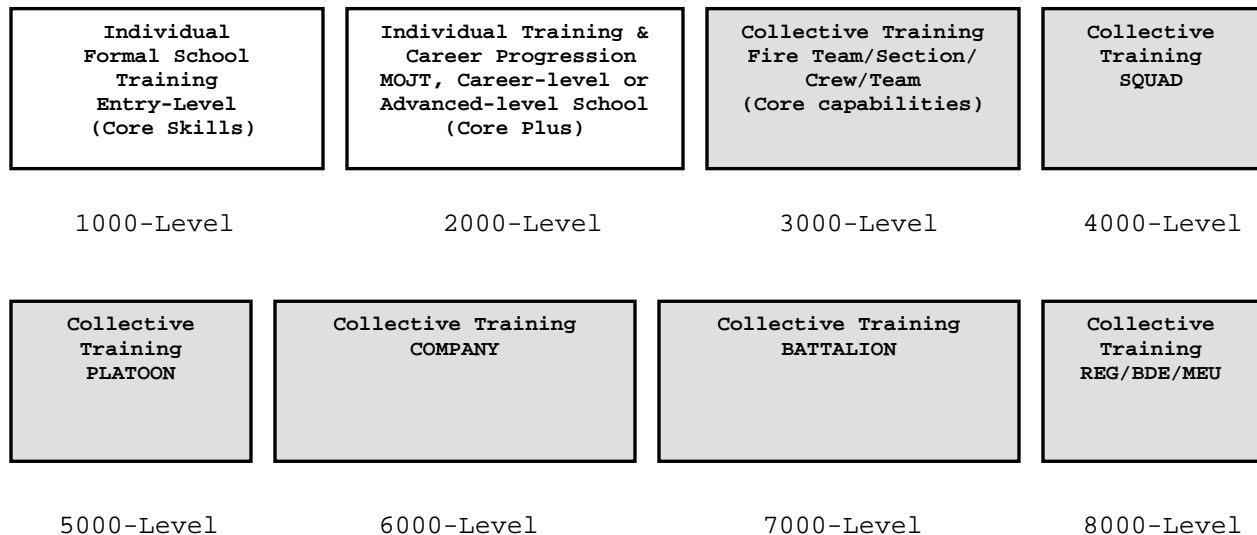


Figure 1-2: T&R Event Levels

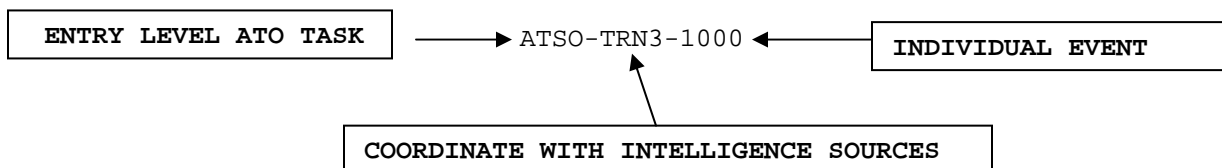


Figure 1-3: T&R Event Coding

1040. EVALUATION-CODED (E-CODED) EVENTS

1. Every unit in the Marine Corps maintains a minimum level of readiness based on a combination of 1000-level training (entry level/Formal School) and individual MOJT, follow-on school training, and the experience of the Marines in the unit. Even units that have never trained together are capable of accomplishing some portion of their mission. Therefore, every unit has a baseline CRP of 40%. Further, only collective events that are critical components of a mission essential task (MET) or are key indicators of a unit's readiness, generate CRP for a MET; these events are "E-coded." Only E-coded events are used to calculate CRP for each MET.

2. Per MCO 1553.1 (Training and Education System), all commanders in the operating forces are required to develop a unit METL based on the Universal Joint Task List (UJTL), Universal Navy Task List (UNTL), Marine Corps Task List (MCTL), doctrine, T/O mission statement, higher headquarters' METLs, contingency plans and the assigned mission. The use of a METL-based training program allows the commander discretion in training and makes the T&R manual a training tool rather than a prescriptive checklist.

3. Typically, not all METs in the T&R Manual will be part of the unit METL. Therefore, only the E-coded events that support the approved METL will be used to calculate a unit's CRP. The commander, based on his assessment of the unit's proficiency and the assigned mission, has the latitude to waive or defer entire METs and/or individual T&R events that support an approved MET. For example, there may be a total of 7 METs in the T&R manual, but only 5 are on the commander's approved METL for his specific unit. Each MET will have a CRP value of 20% (each is 1/5 of 100%); completing the E-coded events for each MET generates CRP. Additionally, if the commander's assessment showed the unit was proficient in a particular E-coded event, he may waive the event; the event is then recorded as completed for CRP calculation. See MCO P3500.72A (Marine Corps Ground T&R Program) for more information on waiving and deferring T&R events.

1050. COMBAT READINESS PERCENTAGE (CRP) CALCULATION

1. Unit training plans shall be designed to accomplish the events that support the unit METL while simultaneously sustaining proficiency in individual core skills. Using the battalion-based (unit) model, the battalion (7000-level) has collective events that directly support a MET on the unit's METL. These collective events are E-coded and are the only events that contribute to unit CRP. This is done to assist commanders in prioritizing the training toward their unit's METL, taking into account resource, time, and personnel constraints.

2. Unit CRP increases after the completion of E-coded events. The number of E-coded events for the MET determines the value of each E-coded event for that particular MET. All E-coded events have equal value for CRP calculation. For example, if there are four e-coded events for a MET, each is worth 25% of MET CRP. If a MET has eight events, then each is worth 12.5%. MET CRP is calculated by adding the percentage of each completed E-coded training event. The percentage for each MET is calculated the same way and all are added together and divided by the number of METs to determine unit CRP. For ease of calculation, we will say that each MET has 4 E-coded events; each contributes 25% towards the completion of the MET. If the unit has completed and three of the four E-coded events for the MET, it has

attained 75% CRP for that MET. The CRP for each MET is added together and divided by the number of METs to get unit CRP; unit CRP is the average of MET CRP.

For Example:

MET 1: 75% (3 OF 4 E-coded events trained)
MET 2: 100% (6 of 6 E-coded events trained)
MET 3: 25% (1 of 4 E-coded events trained)
MET 4: 50% (2 of 4 E-coded events trained)
MET 5: 75% (3 of 4 E-coded events trained)

To get unit CRP, simply add the CRP for each MET and divide by the number of METs:

MET CRP: $75 + 100 + 25 + 50 + 75 = 325$

Unit CRP: $325 \text{ (TOTAL met CRP)} / 5 \text{ (total number of METs)} = 65\%$

1060. T&R EVENT COMPOSITION

This section explains each of the components of a T&R event. These items will be included in all of the events in each T&R manual. Community-based T&R manuals will have several additional components not found in unit-based T&R manuals.

a. **Event Code.** The event code is a 4-4-4 character set:

(1) First 4 characters indicate MOS or Community (AT)

(2) Second 4 characters indicate functional or duty area (e.g., INT, CIP, TRN, etc.)

(3) Third 4 characters indicate the level and sequence (1000 through 8000)

b. **Event Title.** The name of the event.

c. **Event Description.** This is a "yes/no" category to indicate whether or not the event is E-coded. If yes, the event contributes toward CRP of the associated MET. The value of each E-coded event is based on number of E-coded events for that MET. Refer to Section 104 for a more detailed explanation of E-coded events.

d. **Supported MET(s).** List all METs that are supported by the training event.

e. **Sustainment Interval.** This is the period, expressed in number of months, between evaluation or retraining requirements. Skills and capabilities acquired through the accomplishment of training events are to be refreshed at pre-determined intervals. It is essential that these intervals be adhered to in order to ensure the unit and Marines of the unit maintain proficiency.

f. **Billet.** Each individual training event will contain a billet code that designates who (by billet) is responsible for performing that event and

any corresponding formal course required for that billet. Each commander has the flexibility to shift responsibilities based on the organization of his/her command. These codes are based on recommendations from the collective subject matter expertise that developed this manual and are listed for each event. (NOTE: applicable to Community-based T&R manuals only).

g. **Grade.** The rank at which Marines are required to complete the event.

h. **Description:** Description of event purpose, objectives, goals, and requirements. It is a general description of an action requiring learned skills and knowledge (i.e., Engage fixed target with crew-served weapons).

i. **Condition.** The condition(s) set for the real world or combat circumstances in which the tasks are to be performed. They indicate what is provided (i.e., equipment, tools, materials, manuals, aids, etc.), environmental constraints or conditions under which the task is performed, and any specific cues or indicators to which the performer must respond. When resources or safety requirements limit the conditions, this should be stated.

j. **Standard.** The performance standard indicates the basis for judging the effectiveness of the performance. It consists of a carefully worded statement that identifies the proficiency level expected when the task is performed. It is not guidance and shall not be wavered from. Performance standards are specified in terms of accuracy, speed, sequencing, quality of performance, adherence to procedural guidelines, etc.

k. **Event Components/Performance Steps.** Description of the actions that the event is composed of, or a list of subordinate, included T&R event codes and event descriptions. The event components help the user determine what must be accomplished and to properly plan for the event. Event components are used for collective events; performance steps are used for individual events.

l. **Prerequisite Events.** Prerequisites are academic training or other T&R events that must be completed prior to attempting the task. They are lower-level events or tasks that give the individual/unit the skills required to accomplish the event. They can also be planning steps, administrative requirements, or specific parameters that build toward mission accomplishment.

m. **Chained Events.** Collective T&R events are supported by lower-level collective and individual T&R events. This enables unit leaders to effectively identify subordinate T&R events that ultimately support specific mission essential tasks. When the accomplishment of any upper-level events, by their nature, result in the performance of certain subordinate and related events, the events are "chained." The completion of chained events will update sustainment interval credit (and CRP for E-coded events) for the related subordinate level events.

n. **Related ITSS.** A list of all of the Individual Training Standards that support the event.

o. **Initial Training Setting.** All individual events will designate the setting at which the skill is first taught, either at formal school (FS), in the Operational Forces as MOJT, or via a distance learning product (DL).

p. **References.** The training references shall be utilized to determine task performance steps, grading criteria, and ensure standardization of training procedures. They assist the trainee in satisfying the performance standards, or the trainer in evaluating the effectiveness of task completion. Since T&R Manuals provide only a training outline, references are key to developing lesson plans and adding specificity, like performance steps, related doctrine, or other detailed information.

q. **Distance Learning Products.** Examples of distance learning products are Individual Multimedia Instruction (IMI), Computer-Based Training (CBT), Marine Corps Institute (MCI), etc. Included when the event can be taught via one of these media methods vice attending a formal course of instruction or receiving MOJT. (NOTE: applicable to Community-based T&R manuals only).

r. **Support Requirements.** This is a list of the external and internal support the unit and Marines will need to complete the event. This is a key section in the overall T&R effort, as resources will eventually be tied directly to the training towards METs. Future efforts to attain and allocate resources will be based on the requirements outlined in the T&R Manual. The list includes, but is not limited to:

- (1) Range(s)/Training Areas
- (2) Ordnance
- (3) Equipment
- (4) Other Units/Personal

s. **Misc.** Any additional information that will assist in the planning and execution of the event. The list may include, but is not limited to:

- (1) Admin Instructions
- (2) Special Personal Certifications
- (3) Equipment Operating Hours
- (4) Road Miles

1070. UNIT TRAINING

a. The training of Marines to perform as an integrated unit in combat lies at the heart of the T&R program. Unit readiness and individual readiness are directly related. Individual training and the mastery of individual core skills serve as the building blocks for unit combat readiness. A Marine's ability to perform critical skills required in combat is essential; however, it is not necessary to have all individuals within an organization fully trained in order for that organization to accomplish its assigned tasks. Manpower shortfalls, temporary assignments, leave, or other factors outside the commander's control, often affect the ability to conduct individual training. Regardless of current manning, the unit must maintain the ability to accomplish its assigned mission.

b. Commanders will ensure that all tactical training is conducted to a T&R collective training standard (CTS). The T&R manual is to serve as the unit's training plan, and all scheduled training shall support the Unit METL and be tailored to meet T&R standards. Commanders at all levels are responsible for effective combat training. The conduct of training in a professional manner consistent with Marine Corps standards cannot be over emphasized.

c. Commanders shall provide personnel the opportunities to attend formal and operational level courses of instruction as required by this Manual. Attendance at all formal courses must enhance the warfighting capabilities of the unit.

1080. REQUIREMENTS FOR COLLECTIVE TRAINING

Collective training shall serve to achieve standards of unit proficiency required to accomplish wartime missions. Subject to such constraints as safety requirements and limits on space for training, all collective training shall be conducted under conditions and rates of activity closely approximating those that the unit being trained may encounter in combat. When constraints limit the use of realistic training conditions, then simulation and other products of training technology shall be used as applicable to enhance realism. Collective training, to the degree feasible, shall include electronic warfare activity; nuclear, biological, and chemical defense activity; and the periodic use of opposing forces trained in the tactics of potential adversaries. All collective training exercises shall emphasize realistic performance of the functions of individual personnel in the exercising units. Support units shall be intergraded into exercises for realistic training in their wartime supporting roles.

1090. NUCLEAR, BIOLOGICAL, CHEMICAL (NBC) TRAINING

All personnel assigned to the operating force must be trained in Nuclear, Biological, and Chemical Defense (NBCD) in order to survive and continue their mission in an NBC environment. Individual proficiency standards are defined as survival and basic operating standards. Survival standards are those that the individual must master in order to survive NBC attacks. Basic operating standards are those that the individual, and collectively the unit, must be capable of performing to continue operations in an NBC environment. In order to develop and maintain the ability to operate in an NBC environment, NBCD training should be an integral part of the training plan and events in this T&R manual should be trained under NBC conditions whenever possible. All units must be capable of accomplishing their assigned mission in a contaminated environment.

1100. NIGHT TRAINING

While it is understood that all personnel and units of the operating force must be capable of performing their assigned mission in "every clime and place," current doctrine emphasizes the requirement to perform assigned missions at night and during periods of limited visibility. Basic skills are significantly more difficult when visibility is limited. To ensure units are capable of accomplishing their mission at night as well as during the day, they must train under the more difficult limited visibility conditions. As such, all events in this T&R manual should be conducted during the day and at night or under conditions of limited visibility. When there is limited training time available, night training should be conducted in lieu of day training. Due to the nature of terrorist operations and the Tactics, Techniques, and Procedures utilized by terrorists, it is imperative that whenever possible night training be conducted in preparation for antiterrorism operations.

1110. APPLICATION OF SIMULATION

Simulators and other training devices for weapons systems and equipment shall be used when they are capable of effectively and economically supplementing training on the actual equipment. Particular emphasis shall be placed on simulators that provide training that might be limited by safety considerations or constraints on training space, time, or other resources. When deciding on simulation issues, the primary consideration shall be improving the quality of training and consequently the state of readiness. Potential savings in operating and support costs normally shall be an important secondary consideration.

1120. UNIT TRAINING MANAGEMENT

1. Unit Training Management (UTM) is the application of the Systems Approach to Training (SAT) and the Marine Corps Training Principles in a manner that maximizes training results and focuses the training priorities of the unit in preparation for the conduct of its wartime mission.

2. UTM focuses training on the tasks that are essential to a unit's wartime capabilities. The SAT process provides commanders with the requisite tools and techniques to analyze, design, develop, implement and evaluate the training of their unit. The Marine Corps Training Principles provide sound and proven direction and are flexible enough to accommodate the demands of local conditions. These principles are not inclusive, nor do they guarantee success. They are guides that commanders can use to manage unit-training programs. The Marine Corps training principles are:

- (1) Train as you fight
- (2) Make commanders responsible for training
- (3) Use standards-based training
- (4) Use performance-oriented training
- (5) Use mission-oriented training
- (6) Train the MAGTF to fight as a combined arms team
- (7) Train to sustain proficiency
- (8) Train to challenge

3. In order to maintain an efficient, effective training program, it is imperative that commanders at every level fully understand and implement UTM. Guidance for UTM and the process for establishing effective UTM programs are contained in MCO 1553.1 (Training and Education System, MCO 1553.3A (Unit Training Management), and MCRP 3-0A (Unit Training Management Guide).

1130. EVALUATION OF TRAINING

1. Evaluation is a continuous process. Evaluation is integral to training management and is conducted by leaders at every level and during all phases of the planning and conduct of training. Training evaluations measure individual and collective ability to perform events specified in the respective T&R Manuals. To ensure training is efficient and effective, it is imperative that evaluation is an integral part of the training plan.

2. The purpose of formal and informal evaluation is to provide commanders with a process to determine a unit's proficiency in the tasks it must

successfully perform in combat. Informal evaluations should be conducted during every training evolution. Formal evaluations are often scenario-based, focused on the unit's METs, based on collective training standards, and usually conducted during higher-level collective events. MCO P3500.72 (Marine Corps Ground T&R Program) and MCO 1553.1 (Training & Education System) provide further guidance on the conduct of informal and formal evaluations utilizing the Marine Corps Ground T&R Program.

1140. OPERATIONAL RISK MANAGEMENT (ORM)

ORM is a process that enables commanders to plan for and minimize risk while still accomplishing the mission. It is a decision making tool used by Marines at all levels to increase operational effectiveness by anticipating hazards and reducing the potential for loss, thereby increasing the probability of a successful mission. ORM minimizes risks to acceptable levels, commensurate with mission accomplishment. Commanders, leaders, maintainers, planners, and schedulers shall integrate risk assessment in the decision-making process and implement hazard controls to reduce risk to acceptable levels. Applying the ORM process will reduce mishaps, lower costs, and provide for more efficient use of resources. ORM assists the commander in conserving lives and resources and avoiding unnecessary risk, making an informed decision to implement a course of action (COA), identifying feasible and effective control measures where specific measures do not exist, and providing reasonable alternatives for mission accomplishment. Most importantly, ORM assists the commander in determining the balance between training realism and unnecessary risks in training, the impact of training operations on the environment, and the adjustment of training plans to fit the level of proficiency and experience of Marines and leaders. Further guidance for ORM can be found in reference (f).

1150. BILLETS REQUIRING FORMAL SCHOOL ATTENDANCE

As Marines progress through their career, they will be assigned to billets of increasing importance and responsibility. Many of these billets require Marines to attend a follow-on formal school. As the Marine Corps has no Primary or Secondary Military Occupational Specialty (MOS) to designate Antiterrorism Officers (ATO), it utilizes the Billet Designator Antiterrorism Officer (ATO). All Marine Corps Antiterrorism Officers are required to attend Service approved Level II Antiterrorism Officer Training in accordance with MCO 3302.1D.

a. List of DOD approved courses is listed below:

- (1) Service-Approved Level II ATO Training Courses
- (2) Army Resident I US Army MP School, Ft Leonard
Wood, MO (703) 695-8626
- (3) Army MTT/Various Locations FORSCOM (404) 464-5902
- (4) Navy Resident EWTGLANT, Naval Station NW Annex, Chesapeake, VA
(757) 421-8059
- (5) Navy Resident I FLTRANCEN, San Diego, CA (619) 556-7759
- (6) Navy MTT/NCIS MTTLANT, NAB Little Creek, VA (757) 462-8925
- (7) Navy MTT/NCIS MTTPAC, North Island, CA (619) 545-8934
- (8) Navy Resident Navy Reserve, New Orleans, LA (504) 678-7759
- (9) Navy Resident, Military Sealift Command, APMC
Training Center, NJ (732) 938-4979 (Ext. 17)

- (10) Air Force Resident, ACC, Nellis AFB, NV DSN 682-2772
- (11) Air Force Resident, AFRC, Robins USAFB, GA DSN 497-0105
- (12) Air Force Resident, AFSOC, Hurlburt Field, FL DSN 579-1856
- (13) Air Force Resident, AMWC, Ft Dix, NJ DSN 944-4101, ext 187
- (14) Air Force Resident, USAFE, Sembach AB, GE DSN 314-496-6383

b. The MP School will run Mobile Training Teams if funding is provided.

c. FORSCOM is using the USAMPS P0I. They have a series of MTTs planned throughout CONUS.

d. The Navy runs MTTs as needed using NCIS personnel from MTTLANT and MTTTAC.

(NOTE: Commanders may qualify individuals who are subject matter experts and have received formal training in AT and individual protection (e.g., military and/or security police, special agents, etc., who have received specific formal training in AT tactics, techniques, and procedures). These individuals may be individually exempted by the Commander from the Level II ATO Training only if they receive additional training that reviews current AT publications and identifies the methods for obtaining AOR-specific updates.)

1160. ACADEMIC TRAINING

Academic training is pursued after a Marine has completed core skills training at a formal school. It is the portion of individual training that is accomplished by reading pertinent books, manuals, locally created faculty development programs, and/or correspondence materials; or, by attending follow-on or advanced resident courses. The academic training required for each billet is shown bellow in figure 1-4.

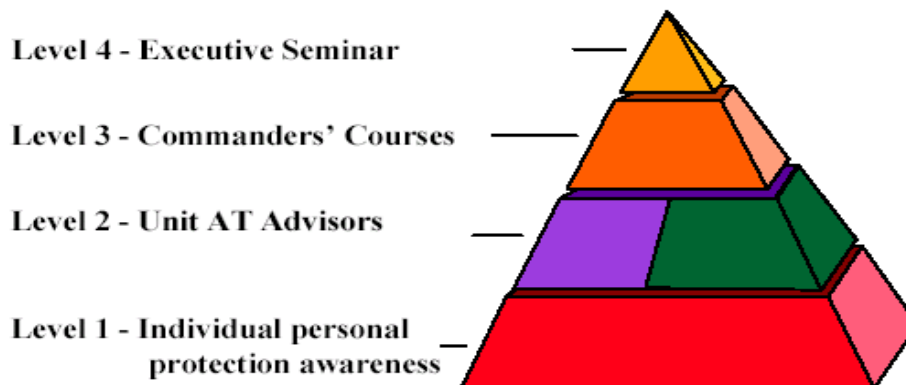


FIGURE 1-4: LEVELS OF AT TRAINING

a. Level I AT Awareness Training

(1) Combatant Commanders and/or Services and/or DoD Agencies shall ensure that every military Service member, DoD employee, and local national hired by the Department of Defense, regardless of rank, is made aware of the

need to maintain vigilance for possible terrorist actions and employ AT tactics, techniques and procedures, as discussed in DoD O-2000.12-H and Joint Pub 3-07.2. Furthermore, the DoD Components shall offer Level I AT Awareness Training to contractor employees, under terms and conditions as specified in the contract.

(2) Family members. Combatant Commanders and/or Services and/or DoD Agencies shall ensure that every family member accompanying DoD personnel overseas is made aware of the need to maintain vigilance for possible terrorist actions and employ AT tactics, techniques, and procedures. Thus, family members 14 years and older (or younger at discretion of the Department of Defense sponsor) traveling beyond CONUS on official business (i.e., on an accompanied permanent change of station move) shall receive Level I AT Awareness Training as part of their pre-departure requirements. Furthermore, the commander should encourage family members to receive Level I AT Awareness Training prior to any OCONUS travel (i.e., leave). Individual security awareness and individual AT training are essential elements of an overall AT program. Each individual must be exposed at the earliest opportunity to share in the responsibility of ensuring alertness and the application of personal protection measures. Therefore, Combatant Commanders and/or Services and/or DoD Agencies shall provide Level I AT Awareness Training in basic training or in general military subject training for all initial-entry Service and DoD Agency personnel.

(3) Thereafter, Combatant Commanders and/or Services and/or DoD Agencies shall provide Level I AT Awareness Training:

(a) Annually to all OCONUS-based DoD personnel.

(b) Annually to all CONUS-based DoD personnel who are eligible for OCONUS deployment.

(c) Active uniformed CONUS-based members of the Combatant Commanders and Services shall receive Level I training annually.

(d) Subsequently, DoD personnel deploying OCONUS shall be provided within 3 months of deployment an AOR update.

(e) Annually to all CONUS-based DoD personnel, regardless of duty status, if the CONUS Terrorism Threat Level is promulgated above "MODERATE."

(f) Individuals may become qualified to administer Level I AT Awareness Training via two methods:

1. Attending a formal Service-approved Level II ATO Training course of instruction. Such training must review current AT publications and identify methods for obtaining AOR-specific terrorism threat analyses, updates, and warnings.

b. AOR-Specific Training Requirements for all Department of Defense Personnel.

(1) Combatant Commanders with geographic responsibilities shall ensure that all DoD personnel entering their AOR have been provided access to AOR-specific information on AT protection.

(2) Combatant Commanders with geographic responsibilities have significant responsibilities for protecting personnel within their AOR. Individuals traveling outside CONUS for either permanent or temporary duty shall have completed annual Level I AT Awareness Training and shall have received a specific AOR update within three months prior to travel.

(3) Combatant Commanders, with geographic responsibilities, shall make AOR-specific AT protection information available to the DoD Components in support of this training. This information may be provided through multiple means including Combatant Commanders publications, messages, and computer homepages. Losing Combatant Commanders and/or Services and/or DoD Agencies shall ensure that personnel departing to another Combatant Commanders geographical AOR shall be exposed to and execute the requirements of the gaining Combatant Commanders AOR update.

(4) Furthermore, to enhance the situational awareness and AT preparedness of units prior to transit through and/or deployment to heightened threat areas, gaining Combatant Commanders with geographic responsibilities shall provide detailed threat information covering transit routes and sites that will be visited by the deployed unit. Such information shall include detailed, focused information on potential terrorist threats (i.e., tailored production and analysis) to aid in the development of tailored AT planning. Since Component Commanders possess organic intelligence and organic or supporting law enforcement resources, institutional knowledge of their AOR and a comprehensive understanding of unit capabilities, they are best suited to provide such information, when augmented or supported by national and theater assets. Combatant Commanders shall ensure that intra-theater transiting units are provided similar information.

c. Level II Antiterrorism Officer (ATO)
Level II ATO Training is designed to produce an AT advisor to the Commander. Combatant Commanders and/or Services and/or DoD Agencies shall ensure that each installation and/or deploying unit (e.g., battalion, squadron, ship) is assigned at least one Level II ATO trained individual.

d. Level III Pre-Command AT Training
Level III Pre-Command AT Training is designed to expose the prospective commander to AT issues. Services and/or DoD Agencies shall ensure that pre-command training tracks provide Level III Pre-Command AT Training to prospective commanders. In particular, this training shall be tailored to provide prospective commanders the depth and breadth of knowledge necessary to perform the full spectrum of AT responsibilities.

e. Level IV AT Executive Seminar
The Level IV AT Executive Seminar is designed to expose senior Officers in the grades of O6-O8 and DoD civilians in equivalent grades to AT issues.

1170. CAREER PROFESSIONAL READING

Marines must continue to strive for excellence in all they do. The career professional reading lists contained in each chapter are finite examples developed by the SMEs who developed this manual of the vast array of materials available for professional and career development. These voluntary reading materials are included to augment core training and help to improve the proficiency of formal school and detachment staff. Although there is no

formal Professional Reading Program established for Antiterrorism Officers, it is recommended that all Antiterrorism Officers subscribe to "The Guardian", a Joint Staff, Deputy Directorate for Antiterrorism/Homeland Defense, Antiterrorism/Force Protection Division Publication.

www.dtic.mil/jcs/force_protection/index.html

Comm: (703) 693-7562

1180. CONCLUSION

The Marine Corps T&R Program continues to evolve. The vision for this program is that it will link the Uniform Joint Task List (UJTL), the Uniform Navy Task List (UNTL), and the Marine Corps Task List (MCTL) to METLs and unit training. In doing so, it will tie all training and training resources directly to unit missions. The Defense Readiness Reporting System (DRRS) is currently being developed and will eventually encompass Enhanced Status of Readiness and Training System (ESCORTS). The purpose of this system is to measure and report on the readiness of military forces and the supporting infrastructure to meet missions and goals assigned by the Secretary of Defense. Training readiness in DRRS will be based primarily on METs. Because unit CRP is based on the unit's training toward its METs, it will provide a more accurate picture of a unit's ability to accomplish its mission. This will give fidelity to future funding requests and factor into the allocation of resources. Additionally, the Ground T&R Program will help to ensure training remains focused on mission accomplishment and that training readiness reporting is tied to commander's METLs.

AT/CIP T&R MANUAL

CHAPTER 2

MISSION ESSENTIAL TASKS

	<u>PARAGRAPH</u>	<u>PAGE</u>
SERVICE LEVEL MISSION ESSENTIAL TASKS MATRIX	2000	2-1

(This page intentionally left blank)

2000. AT/CIP MISSION ESSENTIAL TASK MATRIX

The AT/CIP Mission Essential Task List (METL) Table includes the designated MET number. The following event codes are the linked evaluation coded events that support the MET.

#	SERVICE LEVEL MISSION ESSENTIAL TASK	EVALUATION CODES	EVENTS
1	Provide Intelligence Support to Antiterrorism Operations	AT-INTL-3002 AT-INTL-3004	Estimate the Terrorist Threat Integrate Intelligence Operations
2	Identify and Protect Critical Infrastructure	AT-CIP-8002 AT-CIP-8004 AT-CIP-8005 AT-CIP-8006	Prioritize Assets Perform Vulnerability Analysis and Assessment Conduct Analytical Risk Assessment (RA) Identify Remediation and Countermeasures
3	Conduct Antiterrorism Security Operations	AT-PLAN-3012 AT-OPS-3013	Create Security Plan Coordinate Security Operations
4	Conduct Antiterrorism Training	AT-TRNG-3019 AT-TRNG-3020	Exercise AT Plan Evaluate AT Plan
5	Conduct Antiterrorism Planning	AT-PLAN-3005 AT-PLAN-3007	Develop AT Plan Evaluate AT Plan
6	Conduct Antiterrorism Consequence Management and Incident Mitigation	AT-OPS-3022 AT-PLAN-3016 AT-OPS-3024	Coordinate Consequence-Management Procedures Develop CBRN Post-Incident Response Plan Respond to a Critical Incident

AT/CIP T&R MANUAL

CHAPTER 3

COLLECTIVE TRAINING

	<u>PARAGRAPH</u>	<u>PAGE</u>
PURPOSE	3000	3-1
ADMINISTRATIVE NOTES	3010	3-1
INDEX OF COLLECTIVE TRAINING BY LEVEL	3020	3-2
INDEX OF COLLECTIVE TRAINING BY FUNCTIONAL AREA	3030	3-3
3000-LEVEL COLLECTIVE TRAINING EVENTS	3040	3-4
7000-LEVEL COLLECTIVE TRAINING EVENTS.	3050	3-29
8000-LEVEL COLLECTIVE TRAINING EVENTS.	3060	3-25

(This page intentionally left blank)

AT/CIP T&R MANUAL

CHAPTER 3

COLLECTIVE TRAINING

3000. PURPOSE

This chapter includes all collective training events for Antiterrorism/Critical Infrastructure Protection. A collective event is an event that an established AT Officer would perform in support of a unit. These events are linked to a Service-Level Mission Essential Task (MET). This linkage tailors training for the selected MET. Each collective event is composed of component events that provide the major actions required. This may be likely actions, list of functions, or procedures. Accomplishment and proficiency level required of components events is determined by the event standard.

3010. ADMINISTRATIVE NOTES

T&R events are coded for ease of reference. Each event has a 4-4-4 digit identifier. The first four characters represent the AT billet. The second four characters represent the functional area as listed below.

a. INTL - Intelligence support. Intelligence related to antiterrorism operations such as comprehensive security measures, collection activities, and operations undertaken to guard the force against the effects of enemy action.

b. CIP - Critical Infrastructure Protection. Identification and protection of assets critical to the Defense Transportation System. Loss of a critical asset would result in failure to support the mission of a combatant commander. Assets include worldwide DoD, commercial, and civil physical and command, control, communications, computers, and intelligence infrastructures.

c. PLAN - Planning. AT planning and drafting AT plans and operations orders at all levels.

d. OPS - Operations. The performance of security operations in defense of critical functions, facilities, and forces, to restore order and ensure freedom of movement.

e. TRNG - Training. AT training and exercises, pre-deployment training, training management, development of training plans, and incorporation of lessons learned.

The first number of the final 4 digits represents the organizational level at which the AT/CIP collective event is performed and sequence of the event.

3000 - Fire Team/Section/Team
7000 - Battalion
8000 - Regiment/Brigade/MEU

AT Officers performing duties at the company, platoon or squad level may perform either 3000 or 7000 level tasks, depending upon the situation.

3020. INDEX OF COLLECTIVE EVENTS BY LEVEL

Number	E-Code	Title	Page
		3000 LEVEL	
AT-INTL-3000		Coordinate with intelligence sources	3-4
AT-INTL-3001		Gather all-source intelligence	3-4
AT-INTL-3002	X	Estimate the terrorist threat	3-5
AT-INTL-3003		Write unit-level terrorism assessments	3-6
AT-INTL-3004	X	Integrate intelligence operations	3-6
AT-PLAN-3011	X	Develop the AT plan	3-8
AT-PLAN-3012		Coordinate the logistics assets	3-9
AT-PLAN-3013	X	Evaluate the AT plan	3-10
AT-PLAN-3014		Coordinate unit AT connectivity requirements	3-11
AT-PLAN-3015		Identify resource requirements	3-11
AT-PLAN-3016		Identify post-incident jurisdiction	3-12
AT-PLAN-3017		Coordinate with host nation/local authorities	3-13
AT-PLAN-3018		Establish and maintain an entry control point	3-13
AT-PLAN-3019		Conduct surveillance	3-14
AT-PLAN-3020	X	Develop CBRN post-incident response plan	3-15
AT-PLAN-3021		Identify CBRN pre-incident requirements	3-16
AT-PLAN-3022	X	Create security plan	3-17
AT-OPS-3031	X	Coordinate security operations	3-18
AT-OPS-3032		Coordinate recovery operations	3-18
AT-OPS-3033	X	Coordinate consequence management procedures	3-19
AT-OPS-3034		Activate emergency operations center	3-20
AT-OPS-3035	X	Respond to a critical incident	3-21
AT-TRNG-3041		Conduct awareness education and training	3-23
AT-TRNG-3042	X	Exercise AT plan	3-24
AT-TRNG-3043	X	Evaluate AT plan	3-24
		7000 LEVEL	
AT-CIP-7001		Conduct AT threat assessment	3-26
AT-CIP-7002		Conduct criticality assessment	3-26
AT-CIP-7003		Conduct vulnerability assessment	3-27
AT-CIP-7004		Conduct risk assessment	3-27
		8000 LEVEL	
AT-CIP-8001		Identify critical/key assets	3-30
AT-CIP-8002	X	Prioritize assets	3-30
AT-CIP-8003		Identify key components of a CIP vulnerability assessment	3-32
AT-CIP-8004	X	Perform vulnerability assessment	3-33
AT-CIP-8005		Coordinate with external organizations	3-33
AT-CIP-8006	X	Identify remediation and countermeasures	3-34
AT-CIP-8007	X	Conduct analytical risk assessment	3-35

3030. INDEX OF COLLECTIVE EVENTS BY FUNCTIONAL AREA

Number	E-Code	Title	Page
		INTELLIGENCE	
AT-INTL-3000		Coordinate with intelligence sources	3-4
AT-INTL-3001		Gather all-source intelligence	3-4
AT-INTL-3002	X	Estimate the terrorist threat	3-5
AT-INTL-3003		Write unit-level terrorism assessments	3-6
AT-INTL-3004	X	Integrate intelligence operations	3-6
		PLANNING	
AT-PLAN-3011	X	Develop the AT plan	3-8
AT-PLAN-3012		Coordinate the logistics assets	3-9
AT-PLAN-3013	X	Evaluate the AT plan	3-10
AT-PLAN-3014		Coordinate unit AT connectivity requirements	3-11
AT-PLAN-3015		Identify resource requirements	3-11
AT-PLAN-3016		Identify post-incident jurisdiction	3-12
AT-PLAN-3017		Coordinate with host nation/local authorities	3-13
AT-PLAN-3022	X	Create security plan	3-13
AT-PLAN-3018		Establish and maintain an entry control point	3-14
AT-PLAN-3019		Conduct surveillance	3-15
AT-PLAN-3020	X	Develop CBRN post-incident response plan	3-16
AT-PLAN-3021		Identify CBRN pre-incident requirements	3-17
		OPERATIONS	
AT-OPS-3031	X	Coordinate security operations	3-18
AT-OPS-3032		Coordinate recovery operations	3-18
AT-OPS-3033	X	Coordinate consequence management procedures	3-19
AT-OPS-3034		Activate emergency operations center	3-20
AT-OPS-3035	X	Respond to a critical incident	3-21
		TRAINING	
AT-TRNG-3041		Conduct AT awareness education and training	3-23
AT-TRNG-3042	X	Exercise AT plan	3-24
AT-TRNG-3043	X	Evaluate AT plan	3-24
		CRITICAL INFRASTRUCTURE PROTECTION	
AT-CIP-7001		Conduct AT threat assessment	3-26
AT-CIP-7002		Conduct criticality assessment	3-26
AT-CIP-7003		Conduct vulnerability assessment	3-27
AT-CIP-7004		Conduct risk assessment	3-27
AT-CIP-8001		Identify critical/key assets	3-30
AT-CIP-8002	X	Prioritize assets	3-30
AT-CIP-8003		Identify key components of a CIP vulnerability assessment	3-32
AT-CIP-8004	X	Perform vulnerability assessment	3-33
AT-CIP-8005		Coordinate with external organizations	3-33
AT-CIP-8006	X	Identify remediation and countermeasures	3-34
AT-CIP-8007	X	Conduct analytical risk assessment	3-35

3040. 3000-LEVEL COLLECTIVE TRAINING EVENTS

FUNCTIONAL AREA: INTELLIGENCE SUPPORT

AT-INTL-3000: Coordinate with Intelligence Sources

Evaluation Coded: No

Supported MET(s): 1

Sustainment Interval: 12

Description: Coordinate with internal and external intelligence agencies to integrate and produce intelligence products that will support the units AT/FP Plan.

Condition: Given the required resources and commander's intent, in a tactical or non-tactical situation, during all Force Protection Conditions, as the unit ATO, and with the aid of references.

Standard: Establish a good working relationship with the unit intelligence officer and representatives from external intelligence activities in order to provide integrated and timely intelligence in support of the unit AT/FP plan in accordance with the references.

Component Events:

- Identify organic intelligence assets to support AT operations
- Identify inorganic intelligence assets to support AT operations

References:

DoDD 2000.12, DoD Combating Terrorist Program
DoDINST 2000.14, DoD Combating Terrorism Program Procedures
FM 34-60, Counterintelligence
JP 2-02, National Intelligence Support to Joint Operations
JP 3-07.2, JTTP for Antiterrorism
Marine Corps Intelligence Training and Readiness Manual
MCWP 2-1, Intelligence Operations

AT-INTL-3001: Gather all-source intelligence

Evaluation Coded: No

Supported MET(s): 1

Sustainment Interval: 12

Description: Identify and utilize information sources from all sources, classified and unclassified for the integration of intelligence that will support the units AT/FP Plan.

Condition: Given the required resources and commander's intent, in a tactical or non-tactical situation, during all Force Protection Conditions, as the unit ATO, and with the aid of references.

Standard: State the agencies or units where intelligence information can be gathered in accordance with the references.

Component Events:

- Identify organic intelligence assets to support AT operations

Prerequisite Events:

AT-INTL-3000

References:

DoDD 2000.12, DoD Combating Terrorist Program
DoDINST 2000.14, DoD Combating Terrorism Program Procedures
FM 34-1, Intelligence and Electronic Warfare
FM 34-60, Counterintelligence
Joint Doctrine for Information Operations
JP 2-02, National Intelligence Support to Joint Operations
JP 3-07.2, JTTP for Antiterrorism
Marine Corps Intelligence Training and Readiness Manual

AT-INTL-3002: Estimate the terrorist threat

Evaluation Coded: Yes

Supported MET(s): 1

Sustainment Interval: 12

Description: With the assistance of the Intelligence Officer, develop the terrorist threat estimate.

Condition: Given the required resources and commander's intent, in a tactical or non-tactical situation, during all Force Protection Conditions, as the unit ATO.

Standard: Working in conjunction with the unit intelligence officer, integrate intelligence from organic and inorganic sources and develop the terrorist threat estimate to support the unit AT/FP plan in accordance with the references.

Component Events:

- Identify organic intelligence assets to support AT operations

Prerequisite Events:

AT-INTL-3001

References:

DoDD 2000.12, DoD Combating Terrorist Program
DoDINST 2000.14, DoD Combating Terrorism Program Procedures
FM 34-60, Counterintelligence
JP 2-02, National Intelligence Support to Joint Operations
JP 3-07.2, JTTP for Antiterrorism
Marine Corps Intelligence Training and Readiness Manual
MCWP 2-1, Intelligence Operations

AT-INTL-3003: Write unit-level terrorism assessments

Evaluation Coded: No

Supported MET(s): 1

Sustainment Interval: 12

Description: Coordinate with organic and non-organic sources for required intelligence products in the support of Antiterrorism Operations to acquire intelligence products from organic or non-organic sources.

Condition: Given the required resources, in a tactical or non-tactical situation, during all Force Protection Conditions, as the unit ATO to support the commander's AT plan.

Standard: In accordance with the references.

Prerequisite Events:

AT-INTL-3000 AT-INTL-3001

AT-INTL-3002

References:

DoDD 5200.12-H, Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence

DoDINST 2000.14, DoD Combating Terrorism Program Procedures

FM 34-1, Intelligence and Electronic Warfare

FM 34-60, Counterintelligence

JP 2-01, Joint Intelligence Support to Military Operations

JP 3-07.2, JTTP for Antiterrorism

Marine Corps Intelligence Training and Readiness Manual

MCWP 2-1, Intelligence Operations

ATIS-INTL-3004: Integrate Intelligence Operations

Evaluation Coded: Yes

Supported MET(s): 1

Sustainment Interval: 12

Description: Coordinate with organic and non-organic sources for the integration of intelligence operations that support the units AT/FP Plan and establish effective working relationships to ensure the timely delivery of intelligence products.

Condition: Given the required resources and commander's intent, in a tactical or non-tactical situation, during all Force Protection Conditions, as the unit ATO.

Standard: In accordance with the references and the unit Antiterrorism/Force Protection Plan.

Prerequisite Events:

AT-INTL-3000

References:

DoDD 5200.12-H, Protection of DoD Personnel and Activities Against Acts of

Terrorism and Political Turbulence
DoDINST 2000.14, DoD Combating Terrorism Program Procedures
FM 34-1, Intelligence and Electronic Warfare
FM 34-60, Counterintelligence
JP 2-01, Joint Intelligence Support to Military Operations
JP 3-07.2, JTTP for Antiterrorism
Marine Corps Intelligence Training and Readiness Manual
MCWP 2-1, Intelligence Operations

FUNCTIONAL AREA: PLANNING

AT-PLAN-3011: Develop the AT Plan

Evaluation Coded: Yes

Supported MET(s): 5

Sustainment Interval: 12

Description: Develop AT Plan to support base/deployable units.

Condition: As a unit ATO, given the requirement to develop an AT plan, under any condition, in support of CONUS or OCONUS base/deployable units, and with the aid of references.

Standard: Develop and provide a comprehensive AT plan in support of CONUS or OCONUS base/deployable unit operations, in accordance with the references.

Component Events:

- Conduct a terrorism threat assessment, vulnerability assessment, criticality assessment and risk assessment for the AT Plan.
- Conduct pre-deployment training and AOR briefings for personnel traveling in support of unit deployments.
- Determine appropriate task organization for base/station/deployed forces in CONUS or OCONUS locations.
- Develop command information programs to ensure unit personnel are informed of increased FPCON levels.
- Develop coordinated terrorist incident response and consequence management measures.
- Develop procedures to collect and analyze current terrorist threat information, threat capabilities, and vulnerabilities.
- Develop unit/installation specific random antiterrorism measures.
- Ensure site specific AT measures and RAM's identify and address special security areas.
- Exercise plans annually and review upon completion.
- Identify AT requirements for mass notification of unit's and installation personnel that announces increases in threat levels.
- Identify AT responsibilities of commanders at each level in the chain of command for installation and operational units.
- Identify high-risk personnel/billets for the unit and develop appropriate security measures.
- Obtain legal review of use of force and rules of engagement policies.
- Properly classify AT plans and associated documents.
- Review construction/renovation projects to ensure compliance with the Unified Facilities Criteria.
- Write plans for permanent operations or locations, and incorporate them in operations orders for temporary assigned personnel.

Prerequisite Events:

AT-INTL-3000 AT-INTL-3001
AT-INTL-3002 AT-INTL-3003
AT-INTL-3004 AT-PLAN-3015
AT-PLAN-3016 AT-PLAN-3017
AT-PLAN-3022 AT-OPS-3031
AT-PLAN-3021 AT-OPS-3032
AT-OPS-3033

References:

CJCS 1300.21, Antiterrorism Personal Protection Guide
CJCS 5260, Service Members Self Protection Guide
DoDD 5200.12-H, Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence
DoDD 1300.21, Code of Conduct
DoDD 2000.12, DoD Combating Terrorist Program
DoDI 2000.16, DoD AT Standards
FMFM 7-14, Combating Terrorism
JP 3-07.2, JTTP for Antiterrorism
MCI 02.10b, Terrorism Awareness for Marines
MCO 3302.1D, The Marine Corps Antiterrorism Program
MCRP 3-02E, Individual's Guide for Understanding and Surviving Terrorism
Unified Facilities Construction Criteria Guide

AT-PLAN-3012: Coordinate Logistics Assets

Evaluation Coded: No

Supported MET(s): 5

Sustainment Interval: 12

Description: Unit ATO's must work within the unit staff to coordinate logistics assets in support of the AT plan. Once organic and non-organic assets are identified, the staff must work together to ensure all support is locked-on.

Condition: As the unit ATO, given the requirement to coordinate logistics, a unit AT plan, under any condition and with the aid of references.

Standard: Conduct effective staff coordination to secure logistics assets in support of the unit AT plan in accordance with the references.

Component Events:

- Assess logistical requirements and items available for response to terrorist use of weapons of mass destruction.
- Assist the commander in developing priorities for the distribution of resources.
- Conduct risk, vulnerability, criticality, and other applicable assessments to determine logistical requirements.
- Coordinate/Prioritize input from the AT working group into recommendations for the commander based on the risk, vulnerability, and criticality assessments.
- Determine additional logistics requirements for all FPCONs both stationary and in transit to include requirements for outside agencies and host nation support.
- Determine medical support for AT plan.
- Determine protective equipment, ammunition, and personnel requirements for the security augmentation force.
- Ensure staff planning addresses pre- and post-incident responses to support the AT plan.
- For installation ATOs - develop short- and long-term projects and determine funding avenues available.
- Understand and identify funding sources available to CONUS/OCONUS installation or operational units.

Prerequisite Events:

AT-INTL-3002 AT-INTL-3003
AT-PLAN-3011 AT-PLAN-3014
AT-PLAN-3015 AT-PLAN-3017
AT-PLAN-3021 AT-PLAN-3022
AT-OPS-3033

References:

CJCS 5260, A Self-Help Guide to Antiterrorism
Completed Joint Integrated Vulnerability Assessment
Completed Marine Corps Vulnerability Assessment
DoD 2000.16, DoD AT Standards
DoDD 5200.12-H, Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence
DoDINST 2000.14, DoD Combating Terrorism Program Procedures
HQMC Critical Infrastructure Protection Plan
Inspector General AIRS detailed inspection checklist #480
MCO 3302.1D, The Marine Corps Antiterrorism Program
MCO P5530.14, Marine Corps Physical Security Program Manual
Unified Facilities Construction Criteria Guide

AT-PLAN-3013: Evaluate the AT Plan

Evaluation Coded: Yes

Supported MET(s): 5

Sustainment Interval: 12

Event Description: Conduct a comprehensive review of the AT program in order to facilitate program enhancement, ensure compliance with DoD and Marine Corps AT/FP standards, and ensure the design and implementation of physical security measures coincide with the AT/FP program.

Condition: Given the unit AT/FP Plan, during all Force Protection Conditions, CONUS or OCONUS, as the unit ATO and with the aid of references.

Standard: Ensure all critical staff functions and subordinate unit responsibilities are addressed in the AT Plan and evaluated in accordance with the references.

Component Events:

- ATOs shall routinely review effectiveness of daily AT/FP procedures and physical security measures under the unit AT/FP Plan.
- ATOs will review the unit's AT/FP programs and plans and that of their immediate subordinate (MSC's) in the chain of command.
- AT/FP programs and plans are reviewed to facilitate AT/FP program enhancement, ensure compliance with DoD and Marine Corps AT/FP standards, and ensure the design and implementation of physical security measures coincident with the AT/FP program are consistent with the local terrorism threat level.

Prerequisite Events:

AT-INTL-3001 AT-INTL-3002
AT-INTL-3003 AT-INTL-3004
AT-PLAN-3011 AT-PLAN-3015
AT-OPS-3032 AT-OPS-3033
AT-OPS-3035 AT-TRNG-3042

References:

DoDINST 2000.14, DoD Combating Terrorism Program Procedures
MCO 3302.1B, The Marine Corps Antiterrorism/Force Protection (AT/FP) Program

AT-PLAN-3014: Coordinate Unit AT Connectivity Requirements

Evaluation Code: No

Supported MET(s): 5

Sustainment Interval: 12

Description: Identify AT communication and information system requirements in support of the unit's AT plan in an operational or installation environment based on communication capability.

Condition: As the unit ATO, given the requirement to coordinate communications connectivity, a unit AT plan, under any condition and with the aid of reference.

Standard: Coordinate, test, and evaluate required communications connectivity to support the unit's AT Plan in accordance with the reference.

Component Events:

- Assess the secure/non secure linkage requirements.
- Exercise the unit's communication plan.
- Exercise/Activate the EOC communication plan.
- In coordination with the unit's communication officer establish and test internal/external communications.
- Test and validate externally supported unit communications capabilities with federal, state, and local agencies.

References:

MCO 3302.1B, The Marine Corps Antiterrorism/Force Protection (AT/FP) Program

AT-PLAN-3015: Identify Resource Requirements

Evaluation Coded: No

Supported MET(s): 5

Sustainment Interval: 12

Description: Identify necessary resources to execute the AT Plan and the develop courses of action that will mitigate resource shortfalls.

Condition: As the unit ATO, given the unit AT/FP Plan, during all Force Protection Conditions, under any condition, CONUS or OCONUS, and with the aid of references.

Standard: Identify funds necessary to effectively employ the unit AT plan in accordance with the references.

Component Events:

- Describe AT funding sources.

- Describe areas of the AT program requiring funding.
- Describe how requirements are generated and prioritized.
- Describe research required to support requirements.
- Describe the staffing process involved in funding requirements.

Prerequisite Events:

AT-INTL-3001 AT-INTL-3002
 AT-INTL-3003 AT-PLAN-3011
 AT-PLAN-3013 AT-PLAN-3014
 AT-PLAN-3017 AT-PLAN-3022

References:

MCO 3302.1B, The Marine Corps Antiterrorism/Force Protection (AT/FP) Program
 Unified Facilities Construction Criteria Guide
 USMC Critical Infrastructure Campaign Plan

AT-PLAN-3016: Identify Post-Incident Jurisdiction

Evaluation Coded: No

Supported MET(s): 5

Sustainment Interval: 12

Description: Acting as the ATO, be familiar with agencies and their responsibilities in the post incident investigation and consequence management.

Condition: As the unit ATO, given the unit AT/FP Plan, during all Force Protection Conditions, under any condition, CONUS or OCONUS, and with the aid of references.

Standard: Demonstrate knowledge of lines of jurisdiction, information sharing, and support operations in support of civil, military, and governmental agencies in accordance with the references.

Component Events:

- Develop CBRN consequence management procedures.
- Develop CBRN post incident response plan.
- Coordinate recovery operations.
- Respond to a critical incident.
- Develop alert notification procedures in response to weapons of mass destruction incidents to the National Military Command Authority.
- Coordinate with organic intelligence sources.
- Review installation/unit Memorandums of Understanding/Memorandum of Agreement with local/host agencies.
- Understand references regarding military assistance/support to civil authorities.
- Understand the "No Double Standard Policy."

Prerequisite Events:

AT-PLAN-3012

References:

DoD O-2000.12-H, DoD Antiterrorism Handbook

DoDD 5200.8, Security of Military Installations and Resources
JP 3-10, Joint Doctrine for Rear Area Operations
MCO 3302.1D, The Marine Corps Antiterrorism Program

AT-PLAN-3017: Coordinate with Host Nation/Local Authorities

Evaluation Coded: No

Supported MET(s): 5

Sustainment Interval: 12

Description: Maintain liaison with intelligence agencies and applicable Joint Terrorism Task Force. Clearly define AT operational responsibility and jurisdiction.

Condition: As the unit ATO, given the unit AT/FP Plan, during all Force Protection Conditions, under any condition, CONUS or OCONUS, and with the aid of references.

Standard: Institute and exercise the AT plan in compliance with MOUs/MOAs with host nations or local authorities and per the references.

Component Events:

- Conform to and employ MOU/MOA for local mutual aid support.
- Ensure applicable State Department's force protection instructions are on hand.
- Ensure unit is conforming to jurisdictional agreements in the following areas (SOFA, inter-agency).
- Identify and coordinate information sharing with Joint Terrorism Task Forces.
- Identify organizations with jurisdiction for law enforcement, health, safety, and welfare of assigned service members.

References:

DoDD 5200.8, Security of Military Installations and Resources
DoDINST 2000.14, DoD Combating Terrorism Program Procedures
JP 2-01, Joint Intelligence Support to Military Operations
MCO 3302.1B, The Marine Corps Antiterrorism/Force Protection (AT/FP) Program

AT-PLAN-3018: Establish and Maintain an Entry Control Point

Evaluation Coded: No

Supported MET(s): 3

Sustainment Interval: 6

Description: The entry control point (ECP), as the point of first contact with security forces for those seeking access, is the most critical part in the installation's defense in depth. ECPs include access points to installations, piers, flight-lines, and other restricted areas. It is here that potential terrorists are detected and neutralized.

Condition: Given the required resources, in a tactical or non-tactical situation, during all Force Protection Conditions, as the unit ATO, and with the aid of reference.

Standard: Establish and maintain an Entry Control Point employing all required sentries and posts necessary for successful execution of this security measure in accordance with the reference.

Component Events:

- Coordinate security ops.
- Coordinate logistics.
- Coordinate with host nation/local authorities.

Prerequisite Events:

AT-INTL-3003 AT-PLAN-3011
AT-PLAN-3012 AT-PLAN-3022

References:

MCO 3302.1B, The Marine Corps Antiterrorism/Force Protection (AT/FP) Program

AT-PLAN-3019: Conduct Surveillance

Evaluation Coded: No

Supported MET(s): 3

Sustainment Interval: 6

Description: Before terrorists initiate an attack, they typically conduct months or years of meticulous planning to maximize the likelihood of success. The more sophisticated the operation, such as the attacks of 9/11/01, the more preparation is required. Much of the planning involves gathering exhaustive operational knowledge of a target through surveillance. Terrorists use surveillance to assess capabilities of security systems, judge effectiveness of security measures, and identify security weaknesses. Terrorists closely examine all details of a target, including watch schedules, entry control procedures, periodicity of roving patrols, volume of traffic, citizenship of security guards, and the presence of defensive weapons. Reports of suspicious individuals conducting surveillance of military and civilian sites in the United States and overseas have sharply risen in the past several years. This persistent stream of reports serves as warning that DoD assets and areas are actively being considered as targets of opportunity.

Condition: Given the required resources, in a tactical or non-tactical situation, during all Threat Force Protection Conditions, as the unit ATO, and with the aid of the reference.

Standard: Plan for the conduct of surveillance, employ surveillance detection principles and conduct surveillance to mitigate terrorist threats in accordance with the reference.

Component Events:

- Conduct training on surveillance detection principles.
- Integrate intelligence operations.

Prerequisite Events:

AT-INTL-3001 AT-INTL-3004

References:

MCO 3302.1B, The Marine Corps Antiterrorism/Force Protection (AT/FP) Program

AT-PLAN-3020: Develop CBRN Post-Incident Response Plan

Evaluation Coded: Yes

Supported MET(s): 6

Sustainment Interval: 12

Description: As the unit ATO, assist the unit NBC Officer in the development of the Post-Incident Response Plan. The Post-Incident Response Plan orchestrates the actions of the unit staff and NBC unit to respond effectively to CBRN incidents.

Condition: Given the required resources, in a tactical or non-tactical environment, as a unit or installation ATO, in conjunction with the NBC Officer, and with the aid of references.

Standard: Develop the CBRN Post-incident Response Plan to ensure personnel and assets are prepared to support operations during a Post CBRN event in accordance with the references.

Component Events:

- Advise commander on Threat Level, FPCONs, and countermeasure & RAM development.
- Advise EOC on prevailing weather conditions at the installation.
- Assess terrorist intentions for further attacks of the use of WMD.
- Assist with inventory of damaged assets.
- Assist with the identification of various locations that could serve as alternate command posts.
- Assist with the notification of the installation's population.
- Assist with the reporting of information through appropriate intelligence channels.
- Ensure proper tracking of casualties.
- Ensure CBRN Incident Management Transfer Procedures are developed.
- Ensure CBRN Responder Operational Plan is developed.
- Ensure other installation medical care providers are available to response, as required.
- Maintain security at the incident scene; continue to ensure the safety of personnel.
- Provide recommendation for handling of CBRN fatalities.
- Recover to pre-incident installation baseline status.
- Request funds for un-programmed requirements.

Prerequisite Events:

AT-INTL-3002 AT-INTL-3003
AT-PLAN-3022 AT-PLAN-3015
AT-PLAN-3016 AT-PLAN-3017
AT-PLAN-3021 AT-OPS-3032
AT-OPS-3033

References:

DoDD 2000.12, DoD Combating Terrorist Program
DoDD 2310.2, Personnel Recovery

DoDD 5200.12-H, Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence
DoDD 5200.8, Security of Military Installations and Resources
DoDI 2000.16, DoD AT Standards
DoDI 2310.5, Accounting for Missing Persons
DoDINST 2000.14, DoD Combating Terrorism Program Procedures
JP 3-11, Joint Doctrine for Nuclear Biological and Chemical Defense
MCO 3302.1B, The Marine Corps Antiterrorism Program
MCRP 3-37.2C, Multi-service TTP for NBC Aspects of Consequence Management
MCWP 3-37.2, NBC Protection
USMC Critical Infrastructure Campaign Plan

AT-PLAN-3021: Identify CBRN Pre-Incident Requirements

Evaluation Coded: No

Supported MET(s): 6

Sustainment Interval: 12

Description: Operating as the unit ATO, assist the unit NBC Officer with identifying CBRN Pre-Incident planning and support requirements.

Condition: Given the required resources, in a tactical or non-tactical environment, as a unit or installation ATO, and with the aid of references.

Standard: Identify personnel training requirements and identify and prioritize support assets to ensure that the unit is prepared to support operations during a CBRN event in accordance with the references.

Component Events:

- Assist NBC Officer with disseminating warning information.
- Coordinate/Develop Early-Warning and Mass Notification Procedures.
- Ensure exercises and refresher training is conducted.
- Ensure a collective protection program is established.
- Ensure Mass Casualty Procedures are developed.
- Establish procedures IOT identify key personnel.
- Identify CBRN Table of Organization and Equipment (T/O&E) Requirements.

Prerequisite Events:

AT-INTL-3001 AT-INTL-3003
AT-PLAN-3011 AT-PLAN-3012
AT-PLAN-3014 AT-PLAN-3015
AT-PLAN-3016 AT-PLAN-3017
AT-PLAN-3022 AT-OPS-3031

References:

MCRP 3-37.2C, Multi-service TTP for NBC Aspects of Consequence Management
MCWP 3-37.2, NBC Protection
MCWP 3-37.5, Multi-Service Procedures NBCD of Theater Fixed Sites, Ports and
NTTP 3-07.2.1 (REV A), AT/FP

AT-PLAN-3022: Create Security Plan

Evaluation Coded: Yes

Supported MET(s): 3

Sustainment Interval: 12

Description: A Security Plan is the planned application of resources to mitigate threats to vital assets.

Condition: Given the required resources, in a tactical or non-tactical situation, during all Threat Force Protection Conditions, as the unit ATO, and with the aid of the reference.

Standard: Create a security plan, coordinate support, and utilize all available resources to execute the security plan in accordance with the reference.

Component Events:

- Identify installation command and control relationships.
- Review the installation threat, criticality, vulnerability, and risk assessment.
- Develop physical security measures in support of installation mission requirements.

Prerequisite Events:

AT-INTL-3000 AT-INTL-3002
AT-INTL-3003

References:

MCO 3302.1B, The Marine Corps Antiterrorism/Force Protection (AT/FP) Program

FUNCTIONAL AREA: OPERATIONS

AT-OPS-3031: Coordinate Security Operations

Evaluation Coded: Yes

Supported MET(s): 3

Sustainment Interval: 12

Description: This event demonstrates the ATO's ability to coordinate staff functions and advise the Commanding Officer on the training and employment of forces during Security Operations.

Condition: Given the required resources, in a tactical or non-tactical situation, during all FP Conditions, as the unit ATO and with the aid of the reference.

Standard: Coordinate staff action in regards to the employment of Security Forces in accordance with the reference.

Component Events:

- Coordinate Surveillance Detection Operations.
- Coordinate Personnel Security Details.
- Coordinate Security Force Operations.

Prerequisite Events:

AT-INTL-3000 AT-INTL-3002
AT-INTL-3003 AT-PLAN-3022

References:

MCO 3302.1B, The Marine Corps Antiterrorism/Force Protection (AT/FP) Program

AT-OPS-3032: Coordinate Recovery Operations

Evaluation Coded: No

Supported MET(s): 6

Sustainment Interval: 12

Description: Following an incident, installations or units need to return to a mission ready status as soon as possible. Recovery operations will be those measures taken to restore a unit or installation to operational status. ATO's play an integral role in coordinating the actions associated with recovery operations. ATO's will provide expertise and technical assistance IOT support recovery operations.

Condition: Given the required resources, during all Force Protection Conditions, CONUS or OCONUS, as the unit ATO and with the aid of references.

Standard: Direct and advise supporting and subordinate units on required actions necessary to conduct timely recovery operations in accordance with the references.

Component Events:

- Assist Emergency Operation Center (EOC) requirements.
- Identify requirements for shortfalls in personnel recovery capabilities.

- Implement the Consequence Management Plan.
- Support evacuation plans.
- Support requests for personnel recovery when directed.
- Assist Crisis Management Team (CMT) in planning for and managing multiple and/or diversionary incidents.
- Understand and deal with political, media, and public reaction requirements.

Prerequisite Events:

AT-PLAN-3015 AT-OPS-3033

References:

CJCSI 5261.01B, CBT-RIF
 DoD 7000.14-R, Financial Management
 DoD O-2000.12-H, Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence
 DoDD 2310.2, Personnel Recovery
 DoDD 5200.12-H, Protection of DoD Personnel and Activities Against Acts of
 DoDD 5200.8, Security of Military Installations and Resources
 DoDI 2310.5, "Accounting for Missing Persons"
 MCO 3302.1D, The Marine Corps Antiterrorism Program
 MCO 5740.2F, OPREP-3 SIR Serious Incident Response
 USMC Critical Infrastructure Campaign Plan

AT-OPS-3033: Coordinate Consequence-Management Procedures

Evaluation Coded: Yes

Supported MET(s): 6

Sustainment Interval: 12

Description: As the unit ATO, assist the unit NBC/WMD Officer in developing Consequence-Management Procedures. The unit ATO will provide organic and non-organic support to the NBC/WMD Officer to support decontamination operations and other recovery operations as necessary.

Condition: Given the required resources, in a tactical or non-tactical environment, as a unit or installation ATO, and with the aid of references.

Standard: Coordinate with internal and external support units and agencies and provide assistance to the NBC/WMD Officer during Consequence Management operations in accordance with the references.

Component Events:

- Assess Operational Capability.
- Advise the installation commander on threat.
- Coordinate equipment requests, as required.
- Coordinate the timely/accurate dissemination of information.
- Create Consequence Management Plan and Assess Operational Capability.
- Determine a primary & backup location for the EOC; incorporate collective protection systems in facility.
- Establish installation-centralized command and control facility for EOC.
- Exercise the AT plan.
- Provide continuous coordination/guidance.
- Request funds for un-programmed requirements.

- Update threat assessments based on latest information.

Prerequisite Events:

AT-PLAN-3015 AT-PLAN-3016
AT-PLAN-3017 AT-OPS-3031

References:

AFTTP (I) 3-2.37, Procedures for NBC Aspects of Consequence Management
DoDD 5200.8, Security of Military Installations and Resources
DoDD 5200.8, Security of Military Installations and Resources
JP 3-07.2, JTTP for Antiterrorism
MCO 3302.1D, The Marine Corps Antiterrorism Program
USMC Critical Infrastructure Campaign Plan

AT-OPS-3034: Activate Emergency Operations Center

Evaluation Coded: No

Supported MET(s): 6

Sustainment Interval: 12

Description: The Emergency Operations Center (EOC) is the staff level functional organization that coordinates all activities in response to an incident. The Commanding Officer of the unit or installation, with the ATO acting as primary advisor, will direct incident response from the EOC. The EOC must be manned to provide the primary staff functions of operations, logistics, communications, NBC, intelligence, and administration.

Condition: Given any FPCON or Threat Level, the personnel and equipment to man an Emergency Operations Center, under any condition and with the aid of references.

Standard: Within two hours notice and in accordance with the references.

Component Events:

- Coordinate with First Responders and designated Incident Commander.
- Coordinate with local/state/federal for additional support, as required.
- Ensure EOC ECP is maintained to preclude unauthorized access.
- Ensure a recall procedure of essential personnel has been established.
- Ensure current weather forecasting is provide to the EOC.
- Ensure evacuation routes have been established and identify alternate routes, in event of contaminated routes.
- Ensure Primary and Secondary EOC's locations have been identified.
- Establish communications between the EOC and Incident Commander.
- Identify EOC personnel & a means to alert these personnel.
- Identify locations and capabilities of mass care facilities.
- Initiate request for external augmentation (specialized detection units) if the incident exceeds capabilities.
- Monitor EOC incident information/status boards.
- Support EOC operations.
- Support the development of downwind hazard predictions based on information from the Incident Commander, as required.

References:

DoD O-2000.12-H, Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence
DoDD 5200.8, Security of Military Installations and Resources
DoDINST 2000.14, DoD Combating Terrorism Program Procedures
MCO 3302.1B, The Marine Corps Antiterrorism Program
MCRP 3-02D, Combating Terrorism (FMFM 7-14)
MCRP 3-37.2C, Multi-service TTP for NBC Aspects of Consequence Management

AT-OPS-3035: Respond to a Critical Incident

Evaluation Coded: Yes

Supported MET(s): 6

Sustainment Interval: 12

Description: Critical Incident Response Management is a sequence of command, staff, and first responder actions IOT respond to an incident or other unique events and restore capability. The primary objective of Incident Response Management is to limit the effects, mitigate casualties, and sustain operations. Develop response measures to save lives, protect assets, and prevent further damage to the installation.

Condition: Given the required resources, as the unit ATO, under any condition and with the aid of references.

Standard: Ensure incident response measures include procedures for determining the nature and scope of the incident while coordinating with first responders in order to reconstitute the unit/installation's ability to perform its mission in accordance with the references.

Component Events:

- Identify EOC personnel and a means to alert these personnel.
- Assist with the proper tracking of casualties.
- Begin evacuation procedures, as needed.
- Determine a primary & backup location for the EOC.
- Determine if incident site should be treated as a crime scene (coordinate with security for jurisdiction and handling).
- Determine special controls for delivery of assets into restricted areas.
- Ensure Consequence Management Plan is implemented.
- Ensure Incident Command and Control Procedures are initiated.
- Ensure collective protection systems are incorporated into EOC facility.
- Ensure Crisis Management Plan is executed.
- Ensure MHE is available for emergency clearance of debris for passage of emergency personnel/equipment to incident.
- Ensure PPE is available.
- Ensure the incident site is isolated.
- Ensure weather forecasting is provided to the EOC.
- Provide search and rescue assistance, as directed.
- Report information through appropriate intelligence/law enforcement channels.
- Request funds for un-programmed requirements.

Prerequisite Events:

AT-INTL-3001 AT-PLAN-3011
AT-PLAN-3012 AT-PLAN-3014

AT-PLAN-3015 AT-PLAN-3016
AT-PLAN-3017 AT-PLAN-3022
AT-PLAN-3021 AT-PLAN-3023
AT-OPS-3031 AT-OPS-3032
AT-OPS-3033

References:

CJCSI 5261.01B, CBT-RIF
DoD O-2000.12-H, Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence
DoDD 2000.12, DoD Combating Terrorist Program
DoDD 2310.2, Personnel Recovery
DoDD 5200.8, Security of Military Installations and Resources
FM 3-4, NBC Protection
DoDI 2310.5, Accounting for Missing Persons
JP 3-07.2, JTTP for Antiterrorism

Admin Notes:

Terrorist Incident Response Shared Authorities and Jurisdictions:

- It is customary and usual for military commanders and civilian managers to assume responsibility for initial response, containment, and resolution of criminal incidents that occur on DoD facilities within the United States, its Territories and its possessions.
 - The FBI has lead agency responsibilities for investigation and prosecution of alleged violations of U.S. Code that occur on DoD installations or within DoD facilities. It also has the responsibility for investigating those incidents that an installation commander declares to be "terrorist" in nature. In addition, the FBI has lead agency responsibilities for investigation and prosecution of individuals alleged to have violated the Antiterrorism Act of 1990, Pub. L. 101-519, Sec. 132, November 5, 1990 by committing prohibited acts against Americans abroad.
 - DoD installation military commanders and civilian managers have responsibility and authority for making an initial response, containing, and resolving criminal incidents occurring within their installation.
-

FUNCTIONAL AREA: TRAINING

AT-TRNG-3041: Conduct Awareness Education and Training

Evaluation Coded: No

Supported MET(s): 4

Sustainment Interval: 12

Description: In order to ensure that all personnel in a command are prepared and trained to respond to AT incidents the unit must have a sound training program. To this end the ATO will conduct unit AT Awareness Education and Training.

Condition: During pre-deployment, annual training, during all FP conditions, as the unit ATO and with the aid of references.

Standard: Establish a Unit AT Awareness Education and Training Program and ensure that all personnel receive the training in accordance with the references.

Component Events:

- Conduct Level I training.

References:

DoDD 2000.12, DoD Combating Terrorist Program
DoDI 2000.16, DoD AT Standards
DoDINST 2000.14, DoD Combating Terrorism Program Procedures
JP 3-07.2, JTTP for Antiterrorism
MCO 3302.1B, The Marine Corps Antiterrorism Program

Misc/Admin Note:

- Components Commanders and/or Services and/or DoD Agencies shall ensure that every military Service member, DoD employee, and local national hired by the Department of Defense, regardless of rank, is made aware of the need to maintain vigilance for possible terrorist actions and employ AT tactics, techniques and procedures.
 - The DoD Components shall offer Level I AT Awareness Training to contractor employees, under terms and conditions as specified in the contract.
 - Shall ensure that every family member accompanying DoD personnel overseas is made aware of the need to maintain vigilance for possible terrorist actions and employ AT tactics, techniques, and procedures. Thus, family Members 14 years and older (or younger at discretion of the Department of Defense sponsor) traveling beyond CONUS on official business (i.e., on an accompanied permanent change of station move) shall receive Level I AT Awareness Training as part of their pre-departure requirements. Furthermore, the commander should encourage family members to receive Level I AT Awareness Training prior to any OCONUS travel (i.e., leave). All DoD personnel who are eligible for OCONUS deployment will receive annual Level I training. Active uniformed CONUS-based members of the CINCs and Services shall receive Level I training annually. Subsequently, DoD personnel deploying OCONUS shall be provided within 3 months of deployment an AOR update. Level I training is required for all CONUS-based DoD personnel regardless of duty status.
-

AT-TRNG-3042: Exercise AT Plan

Evaluation Coded: Yes

Supported MET(s): 4

Sustainment Interval: 12

Description: Creation an AT exercise that can be evaluated by measurable standards and includes credible deterrence and response standards; deterrence-specific tactics, techniques and procedures (TTP); terrorist scenarios and hostile intent decision-making. Create Master Event Scenario List (MESL).

Condition: Given the unit AT Plan, during all Force Protection Conditions, CONUS or OCONUS, as the unit ATO and with the aid of references.

Standard: Conduct an AT exercise annually to evaluate the installation's ability to counter or contain a terrorist threat in accordance with the references.

Component Events:

- Conduct field and staff training to exercise AT Plans, to include AT Physical Security measures.

Prerequisite Events:

AT-INTL-3002 AT-INTL-3003
AT-PLAN-3014 AT-PLAN-3015
AT-PLAN-3017 AT-PLAN-3021
AT-PLAN-3022 AT-OPS-3031

References:

DoD O-2000.12-H, Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence
DoDD 2000.12, DoD Combating Terrorist Program
DoDI 2000.16, DoD AT Standards
DoDINST 2000.14, DoD Combating Terrorism Program Procedures
JP 3-07.2, JTTP for Antiterrorism
MCO 3302.1B, The Marine Corps Antiterrorism Program

AT-TRNG-3043: Evaluate AT Plan

Evaluation Coded: Yes

Supported MET(s): 4

Sustainment Interval: 12

Description: This event establishes a comprehensive review of the AT program in order to facilitate program enhancement, ensure compliance with DoD and Marine Corps AT/FP standards, and ensure the design and implementation of physical security measures coincide with the AT/FP program. During the AT exercise, unit leaders and staff members should make note of weaknesses in the AT plan so those items can be discussed during debrief. Debrief items should be written in the item, discussion, recommendation format for easy input into MCLL system. The ATO should consolidate all items of interest and write the AAR. The review process will begin with the AAR developed following the execution of an AT exercise.

Condition: Given the unit AT Plan, the AAR developed from debrief of the AT exercise, during all Force Protection Conditions, CONUS or OCONUS, as the unit ATO and with the aid of references.

Standard: Evaluate the AT plan in accordance with the references.

Component Events:

- Establish measurable standards and include credible deterrence/response, tactics, techniques, and procedures.

Prerequisite Events:

AT-INTL-3002 AT-INTL-3003

AT-PLAN-3011 AT-TRNG-3042

References:

DoDD 2000.12, DoD Combating Terrorist Program

DoDI 2000.16, DoD AT Standards

DoDINST 2000.14, DoD Combating Terrorism Program Procedures

JP 3-07.2, JTTP for Antiterrorism

MCO 3302.1B, The Marine Corps Antiterrorism Program

3050. 7000-LEVEL COLLECTIVE EVENTS

FUNCTIONAL AREA: CRITICAL INFRASTRUCTURE PROTECTION

AT-CIP-7001: Conduct Antiterrorism Threat Assessment

Evaluation Coded: No

Supported MET(s): 2

Sustainment Interval: 12

Description: The AT Risk Management process begins with an assessment of the terrorist threat to DoD personnel and facilities. The AT Threat Assessment is used to identify the terrorist threats posed to DoD assets and/or the threats that could be encountered in executing a mission. This event includes an overview of organizations that provide threat information or analysis to the DoD components. It then describes the analytical approach for assessing terrorist threats, the DoD Threat Methodology, and concludes with a description of how the terrorist threat is assessed at installation or unit level.

Condition: Given the required resources, in a tactical or non-tactical situation, during all FP Conditions, as the unit ATO, and with the aid of references.

Standard: Conduct a threat assessment and advise the Commanding Officer of the results in accordance the references.

Component Events:

- Coordinate with appropriate DoD, Federal and host nation LE/CI agencies.
- Participate as a member of the unit's Threat Working Group.
- Participate as a member of an Emergency Operations Center (EOC) Staff.
- Provides commanders with information on terrorist threats concerning their personnel, facilities, and operations.
- Perform as the liaison to Federal, State, and local agencies as well as host nation agencies to exchange information on terrorists.

Prerequisite Events:

AT-INTL-3000 AT-INTL-3001
AT-INTL-3002

References:

DoD O-2000.12-H, Protection of DoD Personnel and Activities Against Acts Of Terrorism and Political Turbulence

AT-CIP-7002: Conduct Criticality Assessment

Evaluation Coded: No

Supported MET(s): 2

Sustainment Interval: 12

Description: The references describe the methodology commanders and civilian equivalents can use to complete a Criticality Assessment. A critical asset, as defined by DoD Directive 5160.54, is any facility, equipment, service or resource considered essential to DoD operations in peace, crisis, and war;

and warranting measures and precautions to ensure its continued efficient operation, protection from disruption, degradation or destruction, and timely restoration. Critical Assets may be DoD assets or other Government or private assets (e.g., Industrial or Infrastructure Critical Assets (domestic or foreign, whose disruption or loss would render DoD Critical Assets ineffective or otherwise seriously disrupt DoD operations. Critical Assets include both traditional "physical" facilities or equipment, non-physical assets (such as software systems) or "assets" that are distributed in nature (such as command and control networks, wide area networks or similar computer-based networks). Regulations cover items such as VIPs, ammunition storage areas, etc. The Commander's intent extends coverage to other items such as mission critical and high occupancy assets. Critical assets can be people, property, equipment, activities and operations, information, facilities, and materials.

Condition: Given the required resources, in a tactical or non-tactical situation, during all FP Conditions, as the unit ATO, and with the aid of references.

Standard: Conduct a criticality assessment and provide recommendations to the Commander on actions to be taken to mitigate terrorist threats to critical infrastructure in accordance with the references.

Component Events:

- The Criticality Assessment identifies assets supporting DoD missions, units, or activities and deemed critical by military commanders or civilian agency managers.
- For AT purposes, the Criticality Assessment should include high-population facilities, which may not necessarily be mission essential (recreational activities, theaters, or sports venues).
- It addresses the impact of temporary or permanent loss of assets. It examines costs of recovery and reconstitution including time, dollars, capability, and infrastructure support.
- In military units deployed under the command of the Services or a Combatant Command, the staff at each command echelon determines and prioritizes critical assets.
- The Commander responsible for AT approves the prioritized list.
- Identify installation's/units key assets.
- Determine whether critical functions can be duplicated under various attack scenarios.
- Determine time required to duplicate key assets or infrastructures efforts if temporarily or permanently lost.
- Determine priority of response to key assets, functions, and infrastructures in the event of fire, multiple bombings, or other terrorist acts.

Prerequisite Events:

AT-INTL-3002 AT-INTL-3003

References:

DoD O-2000.12-H, Protection of DoD Personnel and Activities Against Acts Of Terrorism and Political Turbulence
DoD Directive 5160.54, Critical Asset Assurance Program

AT-CIP-7003: Conduct Vulnerability Assessment (VA)

Evaluation Coded: No

Supported MET(s): 2

Sustainment Interval: 12

Description: VA is the process the commander uses to determine the susceptibility of assets to attack from threats identified by the AT TA. The VA answers the question "what kind of attack is the asset most/least vulnerable to?" DoD Instruction 2000.16 provides authoritative standards regarding both installation and deploying unit Vulnerability Assessments. Vulnerabilities exist at every installation as a result of the terrorist threat faced. Vulnerabilities are always there, no matter the policies, procedures, structures, and protective equipment. Although terrorist threats cannot be controlled, they can be assessed and the vulnerability of assets to those threats can be mitigated. Identifying and understanding vulnerabilities is important in determining how well an asset shall be protected from loss. Vulnerabilities are also the component of overall risk over which the commander has the most control and greatest influence. By reducing vulnerability, the potential risk to an asset is also reduced.

Condition: Given the required resources, in a tactical or non-tactical situation, during all FP Conditions, as the unit ATO, and with the aid of references.

Standard: Conduct a Vulnerability Assessment and advise the Commander on identified vulnerabilities and actions necessary to mitigate likely threats due to vulnerabilities in accordance with the references.

Component Events:

- The Vulnerability Assessment Process.
- Installation and unit AT officers conduct a VA using key Threat Working Group members in a collaborative effort as the assessment team.
- Teams should include representation from operations, security, intelligence, Counter-intelligence, law enforcement, communications, fire department, engineers, medical services, housing, emergency planning, and WMD planning and response.
- The VA must comply with DoD Instruction 2000.16, "DoD Antiterrorism Standards".

Prerequisite Events:

AT-INTL-3002 AT-INTL-3003

References:

DoD O-2000.12-H, Protection of DoD Personnel and Activities Against Acts Of Terrorism and Political Turbulence
DoDI 2000.16, DoD AT Standards

AT-CIP-7004: Conduct Risk Assessment (RA)

Evaluation Coded: No

Supported MET(s): 2

Sustainment Interval: 12

Description: The RA combines Criticality, Threat, and Vulnerability assessments in order to provide a more complete picture of the risks to an asset or group of assets.

Condition: Given the required resources, in a tactical or non-tactical environment, during all FP Conditions, as the unit ATO and with the aid references.

Standard: Combining the information garnered from the Criticality, Threat, and Vulnerability assessments, develop a risk assessment and brief the commander in accordance with the references.

Component Events:

- The RA is a logical, step-by-step method, and shall require the participation of the entire staff (AT Working Group).
- In starting the RA process, commanders should examine three elements: threat, criticality, and vulnerability.
- Use Risk Assessment Methodology as per the references.
- Describe Risk Assessment.
- Conduct Risk Assessment Practical Exercise.
- Complete the Risk Management Process.

Prerequisite Events:

AT-CIP-7001 AT-CIP-7002
AT-CIP-7003

References:

DoD O-2000.12-H, Protection of DoD Personnel and Activities Against Acts Of Terrorism and Political Turbulence

3060. 8000-LEVEL EVENTS

FUNCTIONAL AREA: CRITICAL INFRASTRUCTURE PROTECTION

AT-CIP-8001: Identify Critical/Key Assets

Evaluation Coded: No

Supported MET(s): 2

Sustainment Interval: 12

Description: Identify the single points of failure for DoD and non-DoD owned critical assets the Marine Corps relies upon in telecommunications, electric power systems, fuel storage and transport, transportation, water supply systems and emergency services. Think critically about these assets, and undertake measures to assure that they are available when needed. The identification of our critical assets and the assessment of there vulnerabilities are crucial to our ultimate goal of achieving mission assurance.

Condition: Given the appropriate resources, as the unit ATO, in any FP condition, and with the aid of references.

Standard: Demonstrate a working knowledge of the 6 CIP protection activities: Analysis and Assessment, Remediation, Monitoring and Reporting, Mitigation, Response, and Reconstitution in accordance with the references.

Component Events:

- Confirm mission and role of organization/unit.
- Identify critical/key assets to be protected, and review the impact if those assets significantly degraded and/or lost. Review both DoD and non-DoD owned assets.
- Value and prioritize assets based on consequences if they were lost.
- Conduct threat and hazard analysis. Identify threats, hazards (natural and man-made) and undesirable events to which each critical asset is exposed, and analyze the expected impact of each threat on each asset.
- Perform a vulnerability analysis and assessment of each critical asset to each specific threat and hazard.
- Develop a report containing individual and collective asset vulnerabilities.
- Ensure agencies are capable of monitoring status of assets.
- Participate in the development of a plan for mitigating and responding to specific threats.
- Participate in the development of a plan for reconstitution of assets.

References:

MCO 3501.36, Marine Corps Critical Infrastructure Protection Program
CJCSI 3209.01, Defense Critical Infrastructure Program (DCIP)
DoDD 3020, Department of Defense Critical Infrastructure Program

AT-CIP-8002: Prioritize Assets

Evaluation Coded: Yes

Supported MET(s): 2

Sustainment Interval: 12

Description:

1. Prioritization of critical assets should be rooted in an analysis of the following areas: Marine Corps missions deemed most critical to national security, as articulated in the National Military Strategy (NMS): The capabilities required to successfully complete those missions: The impact of the loss of any of those critical assets on the successful completion of the mission.

2. Tier definitions of critical asset/infrastructure

Tier I - Assets whose loss or degradation could result in the Warfighter suffering strategic mission failure.

Tier II - Assets whose loss or degradation could result in a sector or element suffering a strategic functional failure, but the Warfighter strategic mission is accomplished.

Tier III - Assets whose loss or degradation could result in individual element failures, but no debilitating strategic mission or core function impacts occur.

Tier IV - Assets not included in Tiers I-III.

Condition: Given the required resources, in a tactical or non-tactical situation, during all FP Conditions, as the unit ATO, and with the aid of references.

Standard: Identify those organic and non-organic key/critical assets that impact Marine Corps mission capabilities in accordance with the references.

Component Events:

- Identify unacceptable risks and risk remediation priorities.
- Identify remediation and counter-measures recommendations, the costs, and conduct trade-offs in a cost-benefit analysis.
- Prioritize the counter-measure and remediation options that address identified risks.
- Obtain acceptance, direction and approval. Recommendations that are approved become the foundation of the CIP/AT/FP plan at the installation or base level.
- Prepare installation CIP/AT/FP plan as a single source document.
- Test, exercise, and validate CIP/AT/FP plan.
- Develop and implement ongoing adjustments to CIP/AT/FP plan.
- Utilize priority levels to reflect impact of asset loss.

Priority Level 1: Loss of the asset will cause a catastrophic loss of capability that cannot be replicated or provided by any other system in less than 120 days.

Priority Level 2: Loss of the asset will cause a severe loss of capability but may be replicated or provided by another system that can be available within 90-120 days.

Priority Level 3: Loss of the asset will cause moderate loss of capability but may be replicated or provided by another system that can be available within 61-89 days.

Priority Level 4: Loss of the asset will cause an intermediate term loss of capability but may be replicate or provided by another system that can be available within 31-60 days.

Priority level 5: Loss of the asset will cause a short-term of capability

that can be replicated or provided by one or more systems within 30 days.

Prerequisite Events:

AT-CIP-8001

References:

MCO 3501.36, Marine Corps Critical Infrastructure Protection Program
CJCSI 3209.01, Defense Critical Infrastructure Program (DCIP)
DoDD 3020, Department of Defense Critical Infrastructure Program

AT-CIP-8003: Identify the key components of a CIP Vulnerability Assessment(VA)

Evaluation Coded: No

Supported MET(s): 2

Sustainment Interval: 12

Description: CIP vulnerability assessment is the process of determining the susceptibility of critical assets, associated infrastructures, or interdependency related single points of failure to adverse conditions. Vulnerability assessments identify weaknesses that can be exploited by threats and recommended specific actions to mitigate the vulnerabilities. Asset susceptibility is defined as an asset that is vulnerable to one of more threats. Associated Infrastructures are supporting assets within the same infrastructure. Asset interdependencies refer to other infrastructures and assets that permit the critical asset to perform its task. Single points of failure are those assets that, if lost, would stop or significantly degrade mission continuity.

Condition: Given the required resources, in a tactical or non-tactical situation, during all FP Conditions, as the unit ATO and with the aid of references.

Standard: Identify those organic and non-organic key/critical assets that impact Marine Corps mission capabilities. The CIP VA should answer the following questions: What are the critical assets for conducting and supporting the mission? If an asset is determined to be critical, is it vulnerable and to what. What can be done to assure the availability of the asset? Successful accomplishment of this event should effectively address these issues in accordance with the references.

Component Events:

- Conduct vulnerability assessment including areas of physical security, cyber security, personnel, supporting infrastructure, supporting materiel and services, and planning and programs.
- Identify vulnerabilities through interviews, physical examination, and cross-walking observation.
- Identify any additional dependencies or previously unidentified redundancies

References:

MCO 3501.36, Marine Corps Critical Infrastructure Protection Program
CJCSI 3209.01, Defense Critical Infrastructure Program (DCIP)
DoDD 3020, Department of Defense Critical Infrastructure Program

AT-CIP-8004: Perform Vulnerability Analysis and Assessment

Evaluation Coded: Yes

Supported MET(s): 2

Sustainment Interval: 12

Description: Installation or unit AT officer's conduct a VA using key Threat Working Group (TWG) members in a collaborative effort as the assessment team. Teams should include representation from operations, security, intelligence, counterintelligence, law enforcement, communications, fire department, engineers, medical services, housing, emergency planning and WMD planning and response. The end-state of the VA process is the identification of physical characteristics or procedures that render critical assets, areas, or special events vulnerable to a range of known or feasible terrorist capabilities. Determination of vulnerability is partly a function of the commander's desired level of protection for the asset, area, or special event. Although performing a detailed VA is not simple, the results quantifying and rating the effectiveness of an installation's current protective measures are invaluable and provide a major tool for developing AT countermeasures.

Condition: Utilizing subordinate units and selected infrastructure representatives, in a tactical or non-tactical situation, during all FP Conditions, as the unit ATO, and with the aid of references.

Standard: Conduct a CIP vulnerability analysis and assessment in accordance with the references.

Component Events:

- List assets and the threats against those assets.
- Determine criteria to be used to assess assets.
- Train assessment team on assessment intent and methodology.
- Assessment Team conducts assessment.
- Consolidate and review assessment results.

Prerequisite Events:

AT-INTL-3001 AT-INTL-3002
AT-CIP-8001

References:

MCO 3501.36, Marine Corps Critical Infrastructure Protection Program
CJCSI 3209.01, Defense Critical Infrastructure Program (DCIP)
DoDD 3020, Department of Defense Critical Infrastructure Program

AT-CIP-8005: Coordinate with external organizations

Evaluation Coded: No

Supported MET(s): 2

Sustainment Interval: 6

Description: This event demonstrates the ATO's ability to coordinate with those external agencies, which provide infrastructure, which directly and/or indirectly supports the Marine Corps.

Condition: Given the required resources, in a tactical or non-tactical situation, during all FP Conditions, as the unit ATO and with the aid of references.

Standard: Establish a CIP Working Group (CIPWG) between Marine Corps and those external agencies that provide infrastructure support and provide a Common Operating Picture (COP) for CIPWG participants in accordance with the references.

Component Events:

- Make liaison with Marine Corps and external agencies that provide infrastructure support.
- Organize these agencies into a CIP Working Group.
- Provide a command-operating picture (COP) for CIPWG.
- Organize memorandum's of understanding/agreement where required.
- Provide threat assessments to CIPWG.

Prerequisite Events:

AT-PLAN-3011 AT-PLAN-3012

References:

MCO 3501.36, Marine Corps Critical Infrastructure Protection Program
CJCSI 3209.01, Defense Critical Infrastructure Program (DCIP)
DoDD 3020, Department of Defense Critical Infrastructure Program

AT-CIP-8006: Identify Remediation and Countermeasures

Evaluation Coded: Yes

Supported MET(s): 2

Sustainment Interval: 12

Description: Once critical assets and infrastructures have been identified by each installation or unit, and their vulnerabilities to a range of threats and hazards assessed, the immediate focus must then shift to identifying countermeasures that can be implemented before undesirable events or attacks occur. The goal is to eliminate known vulnerabilities, and improve the reliability and survivability of those assets. Remedial measures must be the result of integrating several factors, such as relative degree of risk to each asset, the likelihood that specific vulnerabilities will be exploited, and the cost-benefit of a range of proposed counter-measures. Develop a comprehensive risk management approach that looks at interdependencies and interoperability issues in developing and implementing the most appropriate counter-measures and remediation strategies.

Condition: Given the required resources, in a tactical or non-tactical situation, during all FP Conditions, as the unit ATO.

Standard: Utilizing the results of the Criticality Assessment and Risk Assessment, develop remediation and countermeasures to mitigate threats to critical infrastructure in accordance with the references.

Component Events:

- Identify remediation and counter-measures recommendations, the costs, and conduct trade-offs in a cost-benefit analysis.

- Prioritize the counter-measure and remediation options that address identified risks.
- Obtain acceptance, direction and approval. Recommendations that are approved become the foundation of the CIP/AT/FP plan at the installation or base level.
- Prepare installation CIP/AT/FP plan as a single source document.
- Test, exercise, and validate CIP/AT/FP plan.
- Develop and implement ongoing adjustments to CIP/AT/FP plan.

Prerequisite Events:

AT-PLAN-3011 AT-PLAN-3016
 AT-PLAN-3017 AT-PLAN-3022
 AT-CIP-7001 AT-CIP-7002
 AT-CIP-7003 AT-CIP-7004
 AT-CIP-8001 AT-CIP-8003
 AT-CIP-8004

References:

MCO 3501.36, Marine Corps Critical Infrastructure Protection Program
 CJCSI 3209.01, Defense Critical Infrastructure Program (DCIP)
 DoDD 3020, Department of Defense Critical Infrastructure Program

AT-CIP-8007: Conduct Analytical Risk Assessment (RA)

Evaluation Coded: Yes

Supported MET(s): 2

Sustainment Interval: 12

Description: The RA is a logical, step-by-step method, and shall require the participation of the entire staff. In starting the RA process, commanders should examine three elements: threat, criticality (impact loss), and vulnerability.

Condition: Given the required resources, in a tactical or non-tactical situation, during all FP Conditions, as the unit ATO, and with the aid of references.

Standard: Provide the Commander a CIP Risk Assessment based on the asset's vulnerability, criticality and the threat assessment in accordance with the references.

Component Events:

- Consider the installation's mission. How important is that mission to overall U.S. military objectives in the region?
- Consider what resources are available for AT activities on the installation.
- Consider where the nearest available resources are that could augment the installation, should an incident occur.
- Does the Commander have tasking authority for those resources?
- Asset Criticality. Critical assets are determined by both the term and the measure of importance to the installation's mission. Areas that encompass multiple critical assets are referred to as critical areas. The criticality Assessment provides information to prioritize assets and allocate resources to special protective actions.

- Asset vulnerability. A thorough VA shall highlight the susceptibility of a person, group, unit, facility, or asset to a damaging incident.
- The RA and Management process described here does not dictate how to conduct the assessment, nor does it discuss how to identify deficiencies and vulnerabilities. It outlines what type of information to collect and how to organize and display that information for decision-making. If the installation does not have the resident expertise to conduct an AT RA, consider using a JSIVA, and/or Combatant Commander or Service AT assessment reports.

Prerequisite Events:

AT-INTL-3000 AT-INTL-3001
AT-INTL-3002 AT-CIP-8001
AT-CIP-8002 AT-CIP-8003
AT-CIP-8005

References:

MCO 3501.36, Marine Corps Critical Infrastructure Protection Program
CJCSI 3209.01, Defense Critical Infrastructure Program (DCIP)
DoDD 3020, Department of Defense Critical Infrastructure Program

AT/CIP T&R MANUAL

CHAPTER 4

ANTITERRORISM OFFICER INDIVIDUAL TRAINING

	<u>PARAGRAPH</u>	<u>PAGE</u>
PURPOSE	4000	4-3
ADMINISTRATIVE NOTES	4010	4-3
CORE CAPABILITIES	4020	4-3
INDEX OF INDIVIDUAL EVENTS BY FUNCTIONAL AREA	4030	4-4
1000-LEVEL INDIVIDUAL TRAINING EVENTS	4040	4-7

(This page intentionally left blank)

AT/CIP T&R MANUAL

CHAPTER 4

ANTITERRORISM OFFICER INDIVIDUAL TRAINING

4000. PURPOSE

This chapter includes all individual training events for the Antiterrorism Officer (ATO). An individual training standard is an event that an ATO would perform at a unit or installation. These events, like collective events, are linked to a Service-level Mission Essential Tasks (MET). This linkage tailors individual and collective training for the selected MET. Each individual training standard provides an event title, along with the conditions events will be performed under, and the standard to which the event must be performed to be successful.

4010. ADMINISTRATIVE NOTES

1. T&R events are coded for ease of reference. Each event has a 4-4-4-character identifier. The first four characters are "ATO" for Antiterrorism Officer. The second four characters represent the functional area of antiterrorism (AT). The last four characters are the level of training and sequential numbering. Functional area descriptions are as follows:

a. INTL - Intelligence support. Intelligence related to antiterrorism operations such as comprehensive security measures, collection activities, and operations undertaken to guard the force against the effects of enemy action.

b. CIP - Critical Infrastructure Protection. Identification and protection of assets critical to the Defense Transportation System. Loss of a critical asset would result in failure to support the mission of a combatant commander. Assets include worldwide DoD, commercial, and civil physical and command, control, communications, computers, and intelligence infrastructures.

c. PLAN - Planning. AT planning and drafting AT plans and operations orders at all levels.

d. OPS - Operations. The performance of security operations in defense of critical functions, facilities, and forces, to restore order and ensure freedom of movement.

e. TRNG - Training. AT training and exercises, pre-deployment training, training management, development of training plans, and incorporation of lessons learned.

2. The Antiterrorism Officer individual training standards are all 1000 level events, which are taught at the formal school.

4020. CORE SKILLS

1. Coordinate with sources for the integration of intelligence that will support the unit's antiterrorism/force protection (AT/FP) Plan.
2. Coordinate with organic and non-organic sources for the integration of intelligence operations that support the units AT/FP Plan.
3. Coordinate with organic and non-organic sources for required intelligence products in the support of Antiterrorism Operations.
4. Identify information sources for the integration of intelligence that will support the units AT/FP Plan.
5. With the assistance of the Intelligence Officer, determine requirements to develop threat estimate.
6. Identify critical/key assets.
7. Prioritize assets.
8. Identify the key components of a Critical Infrastructure Protection (CIP) vulnerability assessment.
9. Perform vulnerability analysis and assessment.
10. Conduct analytical risk assessment.
11. Identify remediation and countermeasures.
12. Coordinate with external organizations.
13. Conduct antiterrorism threat assessment.
14. Conduct criticality assessment.
15. Conduct vulnerability assessment (VA).
16. Conduct risk assessment (RA).
17. Coordinate Security Operations.
18. Create Security Plan.
19. Exercise AT Plan.
20. Evaluate AT Plan.
21. Conduct awareness Education and Training.
22. Describe the key characteristics of terrorism.
23. Describe individual protective measures against terrorism.
24. Develop AT Plan.
25. Coordinate logistics assets.
26. Evaluate AT Plan.
27. Coordinate unit AT connectivity requirements.
28. Identify resource requirements.
29. Identify post-incident jurisdiction.
30. Coordinate with host nation/local authorities.
31. Coordinate recovery operations.
32. Coordinate consequence-management procedures.
33. Develop Chemical, Biological, Radiological, and Nuclear (CBRN) post incident response plan.
34. Activate emergency operations center.
35. Respond to a critical incident.
36. Identify CBRN (NBC) pre-incident requirements.

4030. INDEX OF INDIVIDUAL TRAINING STANDARDS BY FUNCTIONAL AREA

EVENT	TITLE	PAGE
	INTELLIGENCE	
ATO-INTL-1000	Coordinate with intelligence sources	4-4
ATO-INTL-1001	Gather all-source intelligence	4-4
ATO-INTL-1002	Write unit-level terrorism assessment	4-5
ATO-INTL-1003	Estimate the terrorist threat	4-5
	CRITICAL INFRASTRUCTURE PROTECTION	
ATO-CIP-1010	Identify critical/key assets	4-6
ATO-CIP-1011	Prioritize assets	4-6
ATO-CIP-1012	Identify the key components of a critical infrastructure protection (CIP) vulnerability assessment	4-7
ATO-CIP-1013	Perform vulnerability analysis and assessment	4-7
ATO-CIP-1014	Conduct analytical risk assessment	4-7
ATO-CIP-1015	Identify remediation and countermeasures	4-8
ATO-CIP-1016	Coordinate with external organizations	4-8
ATO-CIP-1017	Conduct antiterrorism threat assessment	4-8
ATO-CIP-1018	Conduct criticality assessment	4-9
ATO-CIP-1019	Conduct vulnerability assessment (VA)	4-9
ATO-CIP-1020	Conduct risk assessment (RA)	4-9
	TRAINING	
ATO-TRNG-1030	Exercise antiterrorism plan	4-11
ATO-TRNG-1031	Evaluate antiterrorism plan	4-11
ATO-TRNG-1032	Conduct AT awareness education and training	4-11
ATO-TRNG-1033	Describe the key characteristics of terrorism	4-12
ATO-TRNG-1034	Describe individual protective measures against terrorism	4-12
	PLANS	
ATO-PLAN-1040	Create security plan	4-13
ATO-PLAN-1041	Develop antiterrorism plan	4-13
ATO-PLAN-1042	Coordinate logistics assets	4-13
ATO-PLAN-1043	Evaluate antiterrorism plan	4-14
ATO-PLAN-1044	Coordinate unit antiterrorism connectivity requirements	4-14
ATO-PLAN-1045	Identify resource requirements	4-15
ATO-PLAN-1046	Identify post incident jurisdiction	4-15
ATO-PLAN-1047	Coordinate with host nation/local authorities	4-15
	OPERATIONS	
ATO-OPS-1060	Coordinate security operations	4-17
ATO-OPS-1061	Coordinate recovery operations	4-17
ATO-OPS-1062	Coordinate consequence-management procedures	4-17
ATO-OPS-1063	Develop CBRN post-incident response plan	4-18
ATO-OPS-1064	Activate emergency operations center	4-18
ATO-OPS-1065	Respond to a critical incident	4-19
ATO-OPS-1066	Identify CBRN pre-incident requirements	4-19

(This page intentionally left blank)

4040. INDIVIDUAL TRAINING EVENTS

FUNCTIONAL AREA: INTELLIGENCE SUPPORT

ATO-INTL-1000: Coordinate with intelligence sources

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the required resources, in a tactical or non-tactical situation, during all Force Protection Conditions, as the unit ATO, in support of the commander's AT/FP Plan, and with the aid of references.

Standard: Make liaison with intelligence sources and provide intelligence inputs to support the unit or installation AT/FP Plan in accordance with the references.

References:

DoDD 2000.12, DoD Combating Terrorist Program
DoDINST 2000.14, DoD Combating Terrorism Program Procedures
FM 34-60, Counterintelligence
JP 2-02, National Intelligence Support to Joint Operations
JP 3-07.2, JTTP for Antiterrorism
Marine Corps Intelligence Training and Readiness Manual
MCWP 2-1, Intelligence Operations

ATO-INTL-1001: Gather all-source intelligence

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the required resources, in a tactical or non-tactical situation, in coordination with the unit Intelligence Officer, during all Force Protection Conditions, in support of the commander's AT/FP Plan as the unit ATO, and with the aid of references.

Standard: Gather all-source intelligence products from organic and inorganic intelligence activities to support the unit AT/FP plan in accordance with the references.

References:

DoDINST 2000.14, DoD Combating Terrorism Program Procedures
FM 34-1, Intelligence and Electronic Warfare
FM 34-60, Counterintelligence
JP 2-01, Joint Intelligence Support to Military Operations
JP 3-07.2, JTTP for Antiterrorism
Marine Corps Intelligence Training and Readiness Manual
MCWP 2-1, Intelligence Operations

ATO-INTL-1002: Write unit-level terrorism assessment

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the required resources, all-source intelligence input, in a tactical or non-tactical situation, during all Force Protection Conditions, as the unit ATO, in coordination with and non-organic intelligence sources, and with the aid of references.

Standard: Conduct a threat assessment to gauge terrorist activities that affect the unit and write a unit-level terrorism assessment in accordance with the references.

References:

DoDINST 2000.14, DoD Combating Terrorism Program Procedures
FM 34-1, Intelligence and Electronic Warfare
FM 34-60, Counterintelligence
JP 2-01, Joint Intelligence Support to Military Operations
JP 3-07.2, JTTP for Antiterrorism
Marine Corps Intelligence Training and Readiness Manual
MCWP 2-1, Intelligence Operations

ATO-INTL-1003: Estimate the terrorist threat

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the required resources, organic, and inorganic intelligence sources, in a tactical or non-tactical situation, in coordination with the unit Intelligence Officer, during all Force Protection Conditions, as the unit ATO, in support of the commander's AT/FP Plan, and in accordance with the references.

Standard: Gather information concerning terrorist cells and activities and estimate the terrorist threat in accordance with the references.

References:

DoDD 2000.12, DoD Combating Terrorist Program
DoDINST 2000.14, DoD Combating Terrorism Program Procedures
FM 34-60, Counterintelligence
JP 2-02, National Intelligence Support to Joint Operations
JP 3-07.2, JTTP for Antiterrorism
Marine Corps Intelligence Training and Readiness Manual
MCWP 2-1, Intelligence Operations

FUNCTIONAL AREA: CRITICAL INFRASTRUCTURE PROTECTION

ATO-CIP-1010: Identify critical/key assets

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the appropriate resources, as the unit ATO, during any Force Protection Condition, and with the aid of references.

Standard: Have a working knowledge of the 6 CIP protection activities: Analysis and Assessment, Remediation, Monitoring and Reporting, Mitigation, Response, and Reconstitution in accordance with the references.

References:

MCO 3501.36, Marine Corps Critical Infrastructure Protection Program
CJCSI 3209.01, Defense Critical Infrastructure Program (DCIP)
DoDD 3020, Department of Defense Critical Infrastructure Program

ATO-CIP-1011: Prioritize assets

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the required resources, in a tactical or non-tactical situation, during all FP Conditions, as the unit ATO, and with the aid of references.

Standard: Reflect impact of asset loss in accordance with the references and priority levels (see administrative notes).

References:

MCO 3501.36, Marine Corps Critical Infrastructure Protection Program
CJCSI 3209.01, Defense Critical Infrastructure Program (DCIP)
DoDD 3020, Department of Defense Critical Infrastructure Program

Administrative Notes:

- Priority Level 1: Loss of the asset will cause a catastrophic loss of capability that cannot be replicated or provided by any other system in less than 120 days.
- Priority Level 2: Loss of the asset will cause a severe loss of capability but may be replicated or provided by another system that can be available within 90-120 days.
- Priority Level 3: Loss of the asset will cause moderate loss of capability but may be replicated or provided by another system that can be available within 61-89 days.
- Priority Level 4: Loss of the asset will cause an intermediate term loss of capability but may be replicated or provided by another system that can be available within 31-60 days.
- Priority level 5: Loss of the asset will cause a short-term of capability that can be replicated or provided by one or more systems within 30 days.

ATO-CIP-1012: Identify the key components of a CIP vulnerability assessment.

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the required resources, in a tactical or non-tactical situation, during all FP Conditions, as the unit ATO, and with the aid of references.

Standard: Identify those organic and non-organic key/critical assets that directly or indirectly impact Marine Corps mission capabilities. The CIP VA should meet the three elements listed in the Administrative Notes.

References:

MCO 3501.36, Marine Corps Critical Infrastructure Protection Program
CJCSI 3209.01, Defense Critical Infrastructure Program (DCIP)
DoDD 3020, Department of Defense Critical Infrastructure Program

Administrative Notes:

1. What are the critical assets for conducting and supporting the mission?
2. If an asset is determined to be critical, is it vulnerable and to what?
3. What can be done to assure the availability of the asset, in accordance with the references.

ATO-CIP-1013: Perform vulnerability analysis and assessment

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the required resources, in a tactical or non-tactical situation, during all FP Conditions, as the unit ATO, and with the aid of references.

Standard: Conduct a CIP Vulnerability Analysis and assessment incorporating the Analysis and Assessment step of the 6 step CIP Protection Activities in accordance with the references.

References:

MCO 3501.36, Marine Corps Critical Infrastructure Protection Program
CJCSI 3209.01, Defense Critical Infrastructure Program (DCIP)
DoDD 3020, Department of Defense Critical Infrastructure Program

ATO-CIP-1014: Conduct analytical risk assessment

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the required resources, in a tactical or non-tactical situation, during all FP Conditions, as the unit ATO, and with the aid of references.

Standard: Provide the Commander a CIP risk assessment based on the asset's vulnerability, criticality and the threat assessment in accordance with the references.

References:

MCO 3501.36, Marine Corps Critical Infrastructure Protection Program
CJCSI 3209.01, Defense Critical Infrastructure Program (DCIP)
DoDD 3020, Department of Defense Critical Infrastructure Program

ATO-CIP-1015: Identify remediation and countermeasures

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the required resources, in a tactical or non-tactical situation, during all FP Conditions, as the unit ATO, and with the aid of references.

Standard: Identify those measures necessary to prevent or mitigate threats identified during the risk assessment in accordance with the references.

References:

MCO 3501.36, Marine Corps Critical Infrastructure Protection Program
CJCSI 3209.01, Defense Critical Infrastructure Program (DCIP)
DoDD 3020, Department of Defense Critical Infrastructure Program

ATO-CIP-1016: Coordinate with external organizations

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the required resources, in a tactical or non-tactical situation, during all FP Conditions, as the unit ATO, and in accordance with the unit Antiterrorism/Force Protection/Critical Infrastructure Plan.

Standard: Establish a CIP Working Group (CIPWG) between Marine Corps and those external agencies that provide infrastructure support. Provide a common operating picture (COP) for CIPWG participants.

References:

MCO 3501.36, Marine Corps Critical Infrastructure Protection Program
CJCSI 3209.01, Defense Critical Infrastructure Program (DCIP)
DoDD 3020, Department of Defense Critical Infrastructure Program

ATO-CIP-1017: Conduct antiterrorism threat assessment

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the required resources, in a tactical or non-tactical situation, during all FP Conditions, as the unit ATO, and with the aid of the reference.

Standard: Conduct and provide the Commander with a threat assessment in accordance with the reference.

References:

DoD O-2000.12-H, DoD Antiterrorism Program

ATO-CIP-1018: Conduct criticality assessment

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the required resources, in a tactical or non-tactical situation, during all FP Conditions, as the unit ATO, and with the aid of the reference.

Standard: Conduct a criticality assessment to identify and prioritized critical infrastructure in accordance with the reference.

References:

DoD O-2000.12-H, DoD Antiterrorism Program

ATO-CIP-1019: Conduct vulnerability assessment (VA)

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the required resources, in a tactical or non-tactical situation, during all FP Conditions, as the unit ATO, and with the aid of references.

Standard: Conduct a Vulnerability Assessment to identify key security issues in regards to critical infrastructure in accordance with the references.

References:

DoD O-2000.12-H, DoD Antiterrorism Program
DoDI 2000.16, DoD AT Standards

ATO-CIP-1020: Conduct risk assessment (RA)

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the required resources, in a tactical or non-tactical situation, during all FP Conditions, as the unit ATO, and with the aid of the reference.

Standard: Conduct a thorough review of the criticality, threat, and vulnerability assessments and identify countermeasures to provide the basis for the risk assessment in accordance with the reference.

References:

DoD O-2000.12-H, DoD Antiterrorism Program

FUNCTIONAL AREA: TRAINING

ATO-TRNG-1030: Exercise AT plan

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the unit AT Plan, during all Force Protection Conditions, CONUS or OCONUS, as the unit ATO, and with the aid of references.

Standard: Conduct an AT exercise at least annually to evaluate the installation's ability to counter or contain a terrorist threat in accordance with the references.

References:

DoD O-2000.12-H, DoD Antiterrorism Program
DoDD 2000.12, DoD Combating Terrorist Program
DoDI 2000.16, DoD AT Standards
DoDINST 2000.14, DoD Combating Terrorism Program Procedures
JP 3-07.2, JTTP for Antiterrorism
MCO 3302.1D, The Marine Corps Antiterrorism Program

ATO-TRNG-1031: Evaluate AT plan

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the unit AT Plan, during all FP Conditions, CONUS or OCONUS, as the unit ATO, and with the aid of references.

Standard: At the conclusion of every AT exercise, provide an AAR for inclusion into the MCCLLS, in accordance with the references.

References:

DoDD 2000.12, DoD Combating Terrorist Program
DoDI 2000.16, DoD AT Standards
DoDINST 2000.14, DoD Combating Terrorism Program Procedures
JP 3-07.2, JTTP for Antiterrorism
MCO 3302.1D, The Marine Corps Antiterrorism Program

ATO-TRNG-1032: Conduct awareness education and training

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: During pre-deployment, and annual training, during all FP conditions, as the unit ATO, and with the aid of references.

Standard: Conduct Level I training for all personnel in accordance with the references.

References:

DoDD 2000.12, DoD Combating Terrorist Program
DoDI 2000.16, DoD AT Standards
DoDINST 2000.14, DoD Combating Terrorism Program Procedures
JP 3-07.2, JTTP for Antiterrorism
MCO 3302.1D, The Marine Corps Antiterrorism Program

ATO-TRNG-1033: Describe the key characteristics of terrorism

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: During pre-deployment and annual training, in all FP conditions, as the unit ATO, and without the aid of references.

Standard: Describe terrorism, the motivation and goals of terrorists, types and characteristics of terrorist groups, organization of terrorist groups and their operations, and define U.S. policy towards terrorism in accordance with the references.

References:

USMC Program of Instruction: Antiterrorism and Force Protection
FMFM 7-14, Combating Terrorism
FMFRP 7-14A, The Individual's Guide for Understanding and Surviving Terrorism
JS GUIDE 5260, Service Member's personal protection Guide: A Self-Help Handbook to Combating Terrorism

ATO-TRNG-1034: Describe individual protective measures against terrorism

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: As the unit ATO and without the aid of references.

Standard: Describe measures, which an individual can take to reduce the risk of being a target of a terrorist act in accordance with the references.

References:

USMC Program of Instruction: Antiterrorism and Force Protection
DoD D 2000.12, DoD Combating Terrorism Program
FMFM 7-14, Combating Terrorism
FMFRP 7-14A, The Individual's Guide for Understanding and Surviving Terrorism
JOINT PUB 3-07.2, Joint Tactics, Techniques, and Procedures for Antiterrorism
JS GUIDE 5260, Service Member's Personal Protection Guide: A Self-Help Handbook to Combating Terrorism
MCO 3302.1, Marine Corps Combating Terrorism Program

FUNCTIONAL AREA: PLANNING

ATO-PLAN-1040: Create security plan

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the required resources, in a tactical or non-tactical situation, during all FP conditions, as the unit ATO, and with the aid of the reference.

Standard: Conduct staff planning and coordinate staff action to create the security plan in accordance with the reference.

References:

MCO 3302.1D, The Marine Corps Antiterrorism Program

ATO-PLAN-1041: Develop AT plan

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: As unit ATO, draft AT plan in support of CONUS or OCONUS base/deployable unit operations, during any FP condition, and with the aid of references.

Standard: Provide a comprehensive AT Plan in support of CONUS or OCONUS base/deployable unit operations, in accordance with the references.

References:

CJCS 5260, Service Members Self Protection Guide
DoD O-2000.12-H, Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence
DoDD 1300.21, Code of Conduct Training and Education
DoDD 1300.7, Training and Education Measures Necessary to Support the Code of Conduct
DoDD 2000.12, DoD Combating Terrorist Program
DoDI 2000.16, DoD AT Standards
FMFM 7-14, Combating Terrorism
JP 3-07.2, JTTP for Antiterrorism
MCI 02.10b, Terrorism Awareness for Marines
MCO 3302.1D, The Marine Corps Antiterrorism Program
MCRP 3-02E, The Individual's Guide for Understanding and Surviving Terrorism
Unified Facilities Construction Criteria Guide

ATO-PLAN-1042: Coordinate logistics assets

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the required resources, as the unit ATO, and with the aid of references.

Standard: Coordinate and plan for logistical support for AT Plans in accordance with the references.

References:

CJCS 5260, A Self-Help Guide to Antiterrorism
Completed Joint Integrated Vulnerability Assessment
Completed Marine Corps Vulnerability Assessment
DoD 2000.16, DoD AT Standards
DoD O-2000.12-H, Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence
DoDINST 2000.14, DoD Combating Terrorism Program Procedures
HQMC Critical Infrastructure Protection Plan
Inspector General AIRS detailed inspection checklist #480
MCO 3302.1D, The Marine Corps Antiterrorism Program
MCO P5530.14, Marine Corps Physical Security Program Manual
Unified Facilities Construction Criteria Guide

ATO-PLAN-1043: Evaluate AT plan

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the unit AT/FP Plan, during all Force Protection Conditions, CONUS or OCONUS, as the unit ATO, and with the aid of references.

Standard: Plan, coordinate, and execute a unit/installation AT exercise to validate the AT Plan in accordance with the references.

References:

DoDINST 2000.14, DoD Combating Terrorism Program Procedures
MCO 3302.1D, The Marine Corps Antiterrorism Program

ATO-PLAN-1044: Coordinate unit AT connectivity requirements

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the mission to maintain communications connectivity for the unit as the ATO and with the aid of the reference.

Standard: Coordinate required connectivity with organic and non-organic communications agencies to support the unit's AT Plan in accordance with the reference.

References:

MCO 3302.1D, The Marine Corps Antiterrorism Program

ATO-PLAN-1045: Identify resource requirements

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the unit AT/FP Plan, during all Force Protection Conditions, CONUS or OCONUS, as the unit ATO, and with the aid of references.

Standard: Identify resource requirements to properly budget for support of the AT Plan in accordance with the references.

References:

MCO 3302.1D, The Marine Corps Antiterrorism Program
Unified Facilities Construction Criteria Guide
USMC Critical Infrastructure Campaign Plan

ATO-PLAN-1046: Identify post-incident jurisdiction

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the unit AT/FP Plan, during all Force Protection Conditions, CONUS or OCONUS, as the unit ATO, and with the aid of references.

Standard: Identify lines of jurisdiction, information sharing, and support operations in support of civil, military, and governmental agencies in accordance with the references.

References:

CJCSM 3150.03, Joint Reporting Structure Event and Incident Reports
DoD O-2000.12-H, DoD Antiterrorism Handbook
DoDD 5200.8, Security of Military Installations and Resources
JP 3-10, Joint Doctrine for Rear Area Operations
MCO 3302.1D, The Marine Corps Antiterrorism Program

ATO-PLAN-1047: Coordinate with host nation/local authorities

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the unit AT/FP Plan, during all Force Protection Conditions, CONUS or OCONUS, as the unit ATO, and with the aid of references.

Standard: In accordance with and in compliance with MOUs/MOAs, and the unit Antiterrorism Plan coordinate with Host Nation/Local Authorities to support the AT Plan in accordance with the references.

References:

DoDD 5200.8, Security of Military Installations and Resources
DoDINST 2000.14, DoD Combating Terrorism Program Procedures

JP 2-01, Joint Intelligence Support to Military Operations
MCO 3302.1D, The Marine Corps Antiterrorism Program

FUNCTIONAL AREA: OPERATIONS

ATO-OPS-1060: Coordinate security operations

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the required resources, in a tactical or non-tactical situation, during all FP Conditions, as the unit ATO, and with the aid of the reference.

Standard: Conduct staff planning and coordinate staff action to employ security operations as necessary in accordance with the reference.

References:

MCO 3302.1D, The Marine Corps Antiterrorism Program

ATO-OPS-1061: Coordinate recovery operations

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the unit AT/FP Plan and required resources, during all Force Protection Conditions, CONUS or OCONUS, as the unit ATO, and with the aid of references.

Standard: Coordinate and conduct those actions necessary, post incident, to restore the unit or installation to a combat ready or operational status, in accordance with the references.

References:

CJCSI 5261.01B, CBT-RIF

DoD 7000.14-R, Financial Management

DoD O-2000.12-H, Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence

DoDD 2310.2, Personnel Recovery

DoDD 5200.12-H, Protection of DoD Personnel and Activities Against Acts of Terrorism

DoDD 5200.8, Security of Military Installations and Resources

DoDI 2310.5, Accounting for Missing Persons

MCO 3302.1D, The Marine Corps Antiterrorism Program

MCO 5740.2F, OPREP-3 SIR Serious Incident Response

USMC Critical Infrastructure Campaign Plan

ATO-OPS-1062: Coordinate consequence-management procedures

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the required resources, in a tactical or non-tactical environment, as a unit or installation ATO, during any FP condition and with the aid of references.

Standard: Coordinate with organic and non-organic units, host-nation/local authorities for support to execute Consequence Management procedures in accordance with the references.

References:

AFTTP (I) 3-2.37, Procedures for NBC Aspects of Consequence Management
DoDD 5200.8, Security of Military Installations and Resources
JP 3-07.2, JTTP for Antiterrorism
MCO 3302.1D, The Marine Corps Antiterrorism Program
USMC Critical Infrastructure Campaign Plan

ATO-OPS-1063: Develop CBRN post-incident response plan

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the required resources, in a tactical or non-tactical environment, as a unit or installation ATO, during any FP condition, and with the aid of references.

Standard: Conduct staff action to ensure personnel and assets are prepared to support operations during a post incident CBRN event in accordance with the references.

References:

DoDD 2000.12, DoD Combating Terrorist Program
DoDD 2310.2, Personnel Recovery
DoDD 5200.12-H, Protection of DoD Personnel and Activities Against Acts of Terrorism
DoDD 5200.8, Security of Military Installations and Resources
DoDI 2000.16, DoD AT Standards
DoDI 2310.5, Accounting for Missing Persons
DoDI 2000.14, DoD Combating Terrorism Program Procedures
JP 3-11, Joint Doctrine for Nuclear Biological and Chemical Defense
MCO 3302.1D, The Marine Corps Antiterrorism Program
MCRP 3-37.2C, Multi-service TTP for NBC Aspects of Consequence Management
MCWP 3-37.2, NBC Protection
USMC Critical Infrastructure Campaign Plan

ATO-OPS-1064: Activate emergency operations center

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: During the Pre-Incident, Increased Readiness, and Response Phases of EOC Operations, as a unit ATO, and with the aid of references.

Standard: During any FPCON or Threat Levels, and within two hours notice, activate a fully functional EOC in accordance with the references.

References:

DoD O-2000.12-H, Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence
DoDD 5200.8, Security of Military Installations and Resources
DoDINST 2000.14, DoD Combating Terrorism Program Procedures
MCO 3302.1D, The Marine Corps Antiterrorism Program
MCRP 3-02D, Combating Terrorism (FMFM 7-14)
MCRP 3-37.2C, Multi-service TTP for NBC Aspects of Consequence Management

ATO-OPS-1065: Respond to a critical incident

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the required resources, as the unit ATO, during any FP condition, and with the aid of references.

Standard: Ensure incident response measures include procedures for determining the nature and scope of the incident while coordinating with first responders in order to reconstitute the unit/installation's ability to perform mission in accordance with the references.

References:

CJCSI 5261.01B, CBT-RIF
DoD 2000.12-H, Protection of DoD Personnel and Activities Against Acts of Terrorism
DoDD 2000.12, DoD Combating Terrorist Program
DoDD 2310.2, Personnel Recovery
DoDD 5200.8, Security of Military Installations and Resources
DoDI 2310.5, Accounting for Missing Persons
DoDINST 2000.14, DoD Combating Terrorism Program Procedures
FM 3-4, NBC Protection
JP 3-07.2, JTTP for Antiterrorism
MCO 3302.1D, The Marine Corps Antiterrorism Program
NTTP 3-07.2.1, (REV A) AT/FP

ATO-OPS-1066: Identify CBRN pre-incident requirements

Initial Training Setting: FS

Grade: SSgt - LtCol

Sustainment Interval: 12

Condition: Given the required resources, in a tactical or non-tactical environment, as a unit or installation ATO, and with the aid of references.

Standard: Conduct staff action to ensure personnel and assets are prepared to support operations during a CBRN event in accordance with the references.

References:

MCRP 3-37.2C, Multi-service TTP for NBC Aspects of Consequence Management

MCWP 3-37.2, NBC Protection

MCWP 3-37.5, Multi-Service Procedures NBCD of Theater Fixed Sites, Ports and Facilities

NTTP 3-07.2.1, (REV A) AT/FP

AT/CIP T&R MANUAL

APPENDIX A

REFERENCES

CJCS 5260, A Self-Help Guide to Antiterrorism
CJCSI 3209.01, Defense Critical Infrastructure Program (DCIP)
CJCSI 5261.01, Combating Terrorism Readiness Initiative Fund
DoD 2000.12-H, Protection of DoD Personnel and Activities
DoD 2000.14, Combating Terrorism Program Procedures
DoDD 3020, Department of Defense Critical Infrastructure Program
DoDD 5200.8, Security of Military Installations and Resources
DoDD 5200.8-R, Physical Security Program
DoDD 5200.12, DoD Combating Terrorist Program
DoDI 1300.21, Code of Conduct Training and Education
DoDI 2000.14, DoD Combating Terrorism Program Procedures
DoDI 2000.16, DoD AT Standards
FM 3-4, NBC Protection
FM 34-1, Intelligence and Electronic Warfare
FM 34-40-9, Direction Finding Operations
FM 34-60, Counterintelligence
FMFM 7-14, Combating Terrorism
JP 2-01, Joint Intelligence Support to Military Operations
JP 3-07.2, JTTP for Antiterrorism
Marine Corps Intelligence Training and Readiness Manual
MCDP 1, Warfighting
MCDP 1-3, Tactics
MCDP 2, Intelligence
MCDP 6, Command and Control
MCRP 3-02D, Combating Terrorism (FMFM 7-14)
MCRP 3-33A, Counter-Guerilla Ops (FMFRP 7-8-3/FM 90-6)
MCRP 4-11B, Military Environment Protection (FM 20-400)
MCI 02.10b, Terrorism Awareness for Marines
MCO 3302.1D, The Marine Corps Antiterrorism Program
MCO 3460.1A, Training and Education Measures Necessary to Support the Code of Conduct
MCO 3501.36, Marine Corps Critical Infrastructure Protection Program
MCO 5500.14A, Flightline Security (FLS) Program
MCO 5740.2F, OPREP-3 SIR Serious Incident Response
MCO P5530.14, Marine Corps Physical Security Program Manual
MCO P5580.2A, Marine Corps Law Enforcement Manual
MCRP 4-11.8C, Handling EPWs
MCRP 5-12.1C, Risk Management
MCWP 2-1, Intelligence Operations
MCWP 3-1, Ground Combat Operations (FMFM 6)
MCWP 3-33, Military Operations Other Than War (MOOTW) Series
SECNAVINST 3300.2A, DON Antiterrorism/Force Protection Program

(This page intentionally left blank)

AT/CIP T&R MANUAL

APPENDIX B

GLOSSARY

Terms in this glossary are subject to change as applicable orders and directives are revised. Terms established by Marine Corps orders or directives take precedence after definitions found in Joint Pub 1-02, *DoD Dictionary of Military and Associated Terms*.

A

After Action Review. A professional discussion of training events conducted after all training to promote learning among training participants. The formality and scope increase with the command level and size of the training evolution. For longer exercises, they should be planned for at predetermined times during an exercise. The results of the AAR shall be recorded on an after action report and forwarded to higher headquarters. The commander and higher headquarters use the results of an AAR to reallocate resources, reprioritize their training plan, and plan for future training.

Assessment. An informal judgment of the unit's proficiency and resources made by a commander or trainer to gain insight into the unit's overall condition. It serves as the basis for the midrange plan. Commanders make frequent use of these determinations during the course of the combat readiness cycle in order to adjust, prioritize or modify training events and plans.

C

Chaining. A process that enables unit leaders to effectively identify subordinate collective events and individual events that support a specific collective event. For example, collective training events at the 4000-level are directly supported by collective events at the 3000-level. Utilizing the building block approach to progressive training, these collective events are further supported by individual training events at the 1000 and 2000-levels. When a higher-level event by its nature requires the completion of lower level events, they are "chained"; Sustainment credit is given for all lower level events chained to a higher event.

Collective Event. A clearly defined, discrete, and measurable activity, action, or event (i.e., task) that requires organized team or unit performance and leads to accomplishment of a mission or function. A collective task is derived from unit missions or higher-level collective tasks. Task accomplishment requires performance of procedures composed of supporting collective or individual tasks. A collective task describes the exact performance a group must perform in the field under actual operational conditions. The term "collective" does not necessarily infer that a unit accomplishes the event. A unit, such as a squad or platoon conducting an attack; may accomplish a collective event or, it may be accomplished by an individual to accomplish a unit mission, such as a battalion supply officer completing a reconciliation of the battalion's CMR. Thus, many collective events will have titles that are the same as individual events; however, the standard and condition will be different because the scope of the collective event is broader.

Collective Training Standards (CTS). Criteria that specify mission and functional area unit proficiency standards for combat, combat support, and combat service support units. They include tasks, conditions, standards, evaluator instruction, and key indicators. CTS are found within collective training events in T&R Manuals.

Combat Readiness Cycle. The combat readiness cycle depicts the relationships within the building block approach to training. The combat readiness cycle progresses from T&R Manual individual core skills training, to the accomplishment of collective training events, and finally, to a unit's participation in a contingency or actual combat. The combat readiness cycle demonstrates the relationship of core capabilities to unit combat readiness. Individual core skills training and the training of collective events lead to unit proficiency and the ability to accomplish the unit's stated mission.

Combat Readiness Percentage (CRP). The CRP is a quantitative numerical value used in calculating collective training readiness based on the E-coded events that support the unit METL. CRP is a concise measure of unit training accomplishments. This numerical value is only a snapshot of training readiness at a specific time. As training is conducted, unit CRP will continuously change.

Component Events. Component events are the major tasks involved in accomplishing a collective event. Listing these tasks guide Marines toward the accomplishment of the event and help evaluators determine if the task has been done to standard. These events may be lower-level collective or individual events that must be accomplished.

Condition. The condition describes the training situation or environment under which the training event or task will take place. Expands on the information in the title by identifying when, where, and why the event or task will occur and what materials, personnel, equipment, environmental provisions, and safety constraints must be present to perform the event or task in a real-world environment. Commanders can modify the conditions of the event to best prepare their Marines to accomplish the assigned mission (e.g. in a desert environment; in a mountain environment; etc.).

Core Competency. Core competency is the comprehensive measure of a unit's ability to accomplish its assigned MET. It serves as the foundation of the T&R Program. Core competencies are those unit core capabilities and individual core skills that support the commander's METL and T/O mission statement. Individual competency is exhibited through demonstration of proficiency in specified core tasks and core plus tasks. Unit proficiency is measured through collective tasks.

Core Capabilities. Core capabilities are the essential functions a unit must be capable of performing during extended contingency/combat operations. Core unit capabilities are based upon mission essential tasks derived from operational plans; doctrine and established tactics; techniques and procedures.

Core Plus Capabilities. Core plus capabilities are advanced capabilities that are environment, mission, or theater specific. Core plus capabilities may entail high-risk, high-cost training for missions that are less likely to be assigned in combat.

Core Plus Skills. Core plus skills are those advanced skills that are environment, mission, rank, or billet specific. 2000-level training is designed to make Marines proficient in core skills in a specific billet or at a specified rank at the Combat Ready level. 3000-8000-level training produces combat leaders and fully qualified section members at the Combat Qualified level. Marines trained at the Combat Qualified level are those the commanding officer feels are capable of accomplishing unit-level missions and of directing the actions of subordinates. Many core plus tasks are learned via MOJT, while others form the base for curriculum in career level MOS courses taught by the formal school.

Core Skills. Core skills are those essential basic skills that "make" a Marine and qualify that Marine for an MOS. They are the 1000-level skills introduced in entry-level training at formal schools and refined in operational units.

D

Defense Readiness Reporting System (DRRS). A comprehensive readiness reporting system that evaluates readiness on the basis of the actual missions and capabilities assigned to the forces. It is a capabilities-based, adaptive, near real-time reporting system for the entire Department of Defense.

Deferred Event. A T&R event that a commanding officer may postpone when in his or her judgment, a lack of logistic support, ammo, ranges, or other training assets requires a temporary exemption. CRP cannot be accrued for deferred "E-coded" events.

Delinquent Event. An event becomes delinquent when a Marine or unit exceeds the sustainment interval for that particular event. The individual or unit must update the delinquent event by first performing all prerequisite events. When the unit commander deems that performing all prerequisite is unattainable, then the delinquent event will be re-demonstrated under the supervision of the appropriate evaluation authority.

E

E-coded Event. An "E-coded" event is a collective T&R event that is a noted indicator of capability or, a noted Collective skill that contributes to the unit's ability to perform the supported MET. As such, only "E-coded" events are assigned a CRP value and used to calculate a unit's CRP.

Entry-level training. Pipeline training that equips students for service with the Marine Operating Forces.

Evaluation. Evaluation is a continuous process that occurs at all echelons, during every phase of training and can be both formal and informal. Evaluations ensure that Marines and units are capable of conducting their combat mission. Evaluation results are used to reallocate resources, reprioritize the training plan, and plan for future training.

Event (Training). (1) An event is a significant training occurrence that is identified, expanded and used as a building block and potential milestone for a unit's training. An event may include formal evaluations. (2) An event within the T&R Program can be an individual training evolution, a collective

training evolution or both. Through T&R events, the unit commander ensures that individual Marines and the unit progress from a combat capable status to a Fully Combat Qualified (FCQ) status.

Event Component. The major procedures (i.e., actions) that must occur to perform a Collective Event to standard.

Exercise Commander (EC). The Commanding General, Marine Expeditionary Force or his appointee will fill this role, unless authority is delegated to the respective commander of the Division, Wing, or FSSG. Responsibilities and functions of the EC include: (1) designate unit(s) to be evaluated, (2) may designate an exercise director, (3) prescribe exercise objectives and T&R events to be evaluated, (4) coordinate with commands or agencies external to the Marine Corps and adjacent Marine Corps commands, when required.

Exercise Director (ED). Designated by the EC to prepare, conduct, and report all evaluation results. Responsibilities and functions of the ED include: (1) Publish a letter of instruction (LOI) that: delineates the T&R events to be evaluated, establishes timeframe of the exercise, lists responsibilities of various elements participating in the exercise, establishes safety requirements/guidelines, and lists coordinating instructions. (2) Designate the TEC and TECG to operate as the central control agency for the exercise. (3) Assign evaluators, to include the senior evaluator, and ensure that those evaluators are properly trained. (4) Develop the general exercise scenario taking into account any objectives/ events prescribed by the EC. (5) Arrange for all resources to include: training areas, airspace, aggressor forces, and other required support.

I

Individual Readiness. The individual training readiness of each Marine is measured by the number of individual events required and completed for the rank or billet currently held.

Individual Training. Training that applies to individual Marines. Examples include rifle qualifications and HMMWV driver licensing.

Individual Training Standards (ITS). Specifies training tasks and standards for each MOS or specialty within the Marine Corps. In most cases, once an MOS or community develops a T&R, the ITS order will be cancelled. However, most communities will probably fold a large portion of their ITS into their new T&R manual.

M

Marine Corps Combat Readiness and Evaluation System (MCCRES). An evaluation system designed to provide commanders with a comprehensive set of mission performance standards from which training programs can be developed; and through which the efficiency and effectiveness of training can be evaluated. The Ground T&R Program will eventually replace MCCRES.

Marine Corps Ground Training and Readiness (T&R) Program. The T&R Program is the Marine Corps' primary tool for planning and conducting training, for planning and conducting training evaluation, and for assessing training readiness. The program will provide the commander with standardized programs of instruction for units within the ground combat, combat support, and combat service support communities. It consolidates the ITS, CTS, METL and other

individual and unit training management tools. T&R is a program of standards that systematizes commonly accepted skills, is open to innovative change, and above all, tailors the training effort to the unit's mission. Further, T&R serves as a training guide and provides commanders an immediate assessment of unit combat readiness by assigning a CRP to key training events. In short, the T&R Program is a building block approach to training that maximizes flexibility and produces the best-trained Marines possible.

Mission Essential Task(s) MET(s). A MET is a collective task in which an organization must be proficient in order to accomplish an appropriate portion of its wartime mission(s). MET listings are the foundation for the T&R manual; all events in the T&R manual support a MET.

Mission Essential Task List (METL). Descriptive training document that provides units a clear, war fighting focused description of collective actions necessary to achieve wartime mission proficiency. The service-level METL, that which is used as the foundation of the T&R manual, is developed using Marine Corps doctrine, Operational Plans, T/Os, UJTL, UNTL, and MCTL. For community based T&R Manuals, an occupational field METL is developed to focus the community's collective training standards. Commanders develop their unit METL from the service-level METL, operational plans, contingency plans, and SOPs.

Mission Performance Standards (MPS). Criteria that specify mission and functional area unit proficiency standards for combat, combat support and combat service support units. They include tasks, conditions, standards, evaluator instruction, and key indicators. MPS are contained within the MCCRES volumes. The MCCRES volumes are being replaced by T&R Manuals. Collective Events will replace MPS.

O

Operational Readiness (DoD, NATO). OR is the capability of a unit/formation, ship, weapon system, or equipment to perform the missions or functions for which it is organized or designed. May be used in a general sense or to express a level or degree of readiness.

P

Performance step. Performance steps are included in the components of an Individual T&R Event. They are the major procedures (i.e., actions) a unit Marine must accomplish to perform an individual event to standard. They describe the procedure the task performer must take to perform the task under operational conditions and provide sufficient information for a task performer to perform the procedure. (May necessitate identification of supporting steps, procedures, or actions in outline form.) Performance steps follow a logical progression and should be followed sequentially, unless otherwise stated. Normally, performance steps are listed only for 1000-level individual events (those that are taught in the entry-level MOS school). Listing performance steps is optional if the steps are already specified in a published reference.

Prerequisite Event. Prerequisites are the academic training and/or T&R events that must be completed prior to attempting the event.

R

Readiness (DoD). Readiness is the ability of US military forces to fight and meet the demands of the national military strategy. Readiness is the synthesis of two distinct but interrelated levels: (a) Unit readiness--The ability to provide capabilities required by combatant commanders to execute assigned missions. This is derived from the ability of each unit to deliver the outputs for which it was designed. (b) Joint readiness--The combatant commander's ability to integrate and synchronize ready combat and support forces to execute assigned missions.

S

Section Skill Tasks. Section Skills are those competencies directly related to unit functioning. They are group rather than individual in nature, and require participation by a section (S-1, S-2, S-3, etc).

Simulation Training. Simulators provide the additional capability to develop and hone core and core plus skills. Accordingly, the development of simulator training events for appropriate T&R syllabi can help maintain valuable combat resources while reducing training time and cost. Therefore, in cases where simulator fidelity and capabilities are such that simulator training closely matches that of actual training events, T&R Manual developers may include the option of using simulators to accomplish the training. CRP credit will be earned for E-coded simulator events based on assessment of relative training event performance.

Standard. A standard is a statement that establishes criteria for how well a task or learning objective must be performed. The standard specifies how well, completely, or accurately a process must be performed or product produced. For higher-level collective events, it describes why the event is being done and the desired end-state of the event. Standards become more specific for lower-level events and outline the accuracy, time limits, sequencing, quality, product, process, restrictions, etc., that indicate the minimum acceptable level of performance required of the event. At a minimum, both collective and individual training standards consist of a task, the condition under which the task is to be performed, and the evaluation criteria that will be used to verify that the task has been performed to a satisfactory level.

Sustainment Training. Periodic retraining or demonstration of an event required maintaining the minimum acceptable level of proficiency or capability required to accomplish a training objective. Sustainment training goes beyond the entry-level and is designed to maintain or further develop proficiency in a given set of skills.

Systems Approach to Training (SAT). An orderly process for analyzing, designing, developing, implementing, and evaluating a unit's training program to ensure the unit, and the Marines of that unit acquire the knowledge and skills essential for the successful conduct of the unit's wartime missions.

T

Training Task. This describes a direct training activity that pertains to an individual Marine. A task is composed of 3 major components: a description of what is to be done, a condition, and a standard.

Technical Exercise Controller (TEC). The TEC is appointed by the ED, and usually comes from his staff or a subordinate command. The TEC is the senior evaluator within the TEGC and should be of equal or higher grade than the commander(s) of the unit(s) being evaluated. The TEC is responsible for ensuring that the evaluation is conducted following the instructions contained in this order and MCO 1553.3A. Specific T&R Manuals are used as the source for evaluation criteria.

Tactical Exercise Control Group (TEGC). A TEGC is formed to provide subject matter experts in the functional areas being evaluated. The benefit of establishing a permanent TEGC is to have resident, dedicated evaluation authority experience, and knowledgeable in evaluation technique. The responsibilities and functions of the TEGC include: (1) developing a detailed exercise scenario to include the objectives and events prescribed by the EC/ED in the exercise LOI; (2) conducting detailed evaluator training prior to the exercise; (3) coordinating and controlling role players and aggressors; (4) compiling the evaluation data submitted by the evaluators and submitting required results to the ED; (5) preparing and conducting a detailed exercise debrief for the evaluated unit(s).

Training Plan. Training document that outlines the general plan for the conduct of individual and collective training in an organization for specified periods of time.

U

Unit CRP. Unit CRP is a percentage of the E-coded collective events that support the unit METL accomplished by the unit. Unit CRP is the average of all MET CRP.

Unit Evaluation. All units in the Marine Corps must be evaluated, either formally or informally, to ensure they are capable of conducting their combat mission. Informal evaluations should take place during all training events. The timing of formal evaluations is critical and should, when appropriate, be directly related to the units' operational deployment cycle. Formal evaluations should take place after the unit has been staffed with the majority of its personnel, has had sufficient time to train to individual and collective standards, and early enough in the training cycle so there is sufficient time to correctly identified weaknesses prior to deployment. All combat units, and units task organized for combat require formal evaluations prior to operational deployments.

Unit Training Management (UTM). Unit training management is the use of the SAT and Marine Corps training principles in a manner that maximizes training results and focuses the training priorities of the unit on its wartime mission. UTM governs the major peacetime training activity of the Marine Corps and applies to all echelons of the Total Force.

W

Waived Event. An event that is waived by a commanding officer when in his or her judgment, previous experience or related performance satisfies the requirement of a particular event.

(This page intentionally left blank)

AT/CIP T&R MANUAL

APPENDIX C

ANTITERRORISM DEFINITIONS

Antiterrorism (AT). Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces.

AT Officer (ATO). The installation, base, regional, facility, or deploying unit AT advisor charged with managing the AT Program.

AT Plan. The specific measures taken to establish and maintain an AT Program.

AT Planning. The process of developing specific guidance and execution oriented instructions for subordinates.

AT Program. One of several security-related programs that fall under the overarching Combating Terrorism (CbT) programs that is a collective, proactive effort focused on the prevention and detection of terrorist attacks against DoD personnel, their families, facilities, installations, and infrastructure critical to mission accomplishment as well as the preparation to defend against and planning for the response to the consequences of terrorist incidents. Although not elements of AT, plans for terrorism consequence management preparedness and response measures as well as plans for continuing essential military operations are important adjuncts to an effective AT program. The minimum elements of an AT program are AT risk management, planning, training and exercises, resource generation, and program reviews.

AT Resource Generation. The process used to identify and submit requirements through existing DoD Planning, Programming, Budgeting and Execution (PPBE), CbT-Combating Terrorism Readiness Initiatives Fund (CbT-RIF), and other funding mechanisms. Central to success of resource generation is tracking, and then funding identified AT program life-cycle costs and assessed shortfalls to mitigate risk associated with terrorist capabilities.

AT Risk Management. The process of systematically identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits. The end products of the AT program risk management process shall be the identification of areas and assets that are vulnerable to the identified threat attack means. From the assessment of risk based upon the three critical components of AT risk management (TA, asset criticality assessment, and VA), the Commander must determine which assets require the most protection and where future expenditures are required to minimize risk of attack or lessen the severity of the outcome of an attack. The Commander must decide on how best to employ given resources and AT force protection measures to deter, mitigate, or prepare for a terrorist incident.

AT Threat Assessment. The process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat. Also, it is a product of a threat analysis for a particular unit, installation, or activity.

AT Training. The development of individual, leader, and collective skills as well as conducting comprehensive exercises to validate plans for antiterrorism, incident response, consequence management, and continuity of essential military operations.

AT VA. A DoD, command, or unit-level evaluation (assessment) to determine the vulnerability of an installation, unit, exercise, port, ship, residence, facility, or other site to a terrorist attack. Identifies areas of improvement to withstand, mitigate, or deter acts of violence or terrorism. The process the commander uses to determine the susceptibility to attack from the full range of threats to the security of personnel, family members, and facilities, which provide a basis for determining antiterrorism measures that can protect personnel and assets from terrorist attacks.

Combating Terrorism (CbT). In the Department of Defense all actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts), counter terrorism (offensive measures taken to prevent (preempt), deter (disrupt), and respond to terrorism), terrorism consequence management (preparation for and response to the consequences of a terrorist incident/event), and intelligence support (collection and dissemination of terrorism-related information), taken to oppose terrorism throughout the entire threat spectrum, including terrorist use of chemical, biological, radiological, nuclear materials, or high-yield explosive (CBRNE) devices.

Combating Terrorism Readiness Initiatives Fund (CbT-RIF). Program established by Congress and managed by the Joint Staff (J-3) that provides funds for emergency or unforeseen high priority Force Protection projects or equipment submitted by the Commanders of the Combatant Commands and approved by the Chairman of the Joint Chiefs of Staff.

Commander. Any commanding officer, installation commander, or other command authority, or civilian supervisor in a comparable position.
Consequence Management. Those measures taken to protect public health and safety, restore essential government services, and provide emergency relief to Governments, businesses, and individuals affected by the consequences of a CBRNE situation. For domestic consequence management, the primary authority rests with the States to respond and the Federal Government through the Department of Homeland Security as the primary Federal Agency to provide assistance as required. The Department of State is the primary Federal Agency for Foreign Consequence Management.

Critical Asset. Any facility, equipment, service or resource considered essential to DoD operations in peace, crisis, and war and warranting measures and precautions to ensure its continued efficient operation, protection from disruption, degradation, or destruction, and timely restoration. Critical assets may be DoD assets or other government or private assets, (e.g. industrial or infrastructure critical assets), domestic or foreign, whose disruption or loss would render DoD critical assets ineffective or otherwise seriously disrupt DoD operations. Critical assets include traditional "physical" facilities and equipment, non-physical assets (such as software systems), or "assets" that are distributed in nature (such as command and control networks, wide area networks or similar computer-based networks).

Critical Infrastructure. Infrastructure deemed essential to DoD operations or the functioning of a Critical Asset.

Critical Infrastructure Protection. DoD program to identify and protect assets critical to the Defense Transportation System. Loss of a critical asset would result in a failure to support the mission of a combatant commander. Assets include worldwide DoD, commercial and civil physical and command, control, communications, computers, and intelligence infrastructures.

Defense Contractor. Any individual, firm, corporation, partnership, association, or other legal non-Federal entity that enters into a contract directly with the Department of Defense to furnish services, supplies, or both, including construction. Thus, Defense contractors may include U.S. nationals, local citizens, or third country nationals. Defense contractors do not include foreign governments or representatives of foreign governments that are engaged in selling to the Department of Defense or a DoD Component or foreign corporations wholly owned by foreign governments.

Defense Criminal Investigative Organizations (DCIO). The U.S. Army Criminal Investigation Command (USACIDC), the Naval Criminal Investigative Service (NCIS), the Air Force Office of Special Investigations (AFOSI), and the Defense Criminal Investigative Service (DCIS) are the four DoD law enforcement organizations that make up the DCIOs. These agencies have law enforcement investigative responsibilities for federal felony offenses committed against the DoD and its Military Branches and are all members of the regional Joint Terrorism Task Forces (JTTF) and the National-JTTF.

Duress System. A system that can covertly communicate a situation of duress (hostile, hostage, security compromised) to a security control center, or to other personnel who can notify a security control center.

Emergency CbT-RIF Requirement. An unanticipated requirement created by a combination of circumstances or the resulting state that requires immediate action to prevent, deter, or respond to a terrorist act.

Emergent CbT-RIF Requirement. A newly formed, unexpected requirement resulting from a logical consequence of unforeseen circumstances calling for prompt action.

Family Member. Individuals defined as "dependent" in Section 1072(2) of 10 U.S.C (reference (f)). Includes spouses, unmarried widows, unmarried widowers; unmarried legitimate children, including adopted children or stepchildren, who are under 21, incapable of self-support or under 23 and enrolled in a full time education institution.

Force Protection (FP). Actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease.

FP Conditions (FPCONS). A DoD-approved system that standardizes the Departments' identification and recommended preventive actions and responses to terrorist threats against U.S. personnel and facilities. This system is the principle means for a commander to apply an operational decision on how

to protect against terrorism and facilitates inter-Service coordination and support for antiterrorism activities.

High-Risk Billet. Authorized personnel billet (identified and recommended by appropriate authority) that because of grade, assignment, travel itinerary or symbolic value may make personnel filling them an especially attractive or accessible terrorist target.

Law Enforcement and Counterintelligence Community (LECIC). The USACIDC, U.S. Army Military Intelligence (MI), NCIS, AFOSI, and DCIS include the Department of Defense's law enforcement and counterintelligence investigative community. These agencies are responsible for law enforcement liaison and interaction with local, State, and Federal law enforcement agencies, including the FBI.

Protective Service Operations (PSO). PSO entails the protection of dignitaries and other high-risk personnel in the combatant commander's area of responsibility where significant threats exist. Those threats include assaults, kidnappings, assassinations, and attempts to embarrass the U.S. Government. These conditions may result in the requirement to provide increased safety and security through the assignment of protective service details.

Radiological Material. Radioactive material usually found in research, industrial or medical applications or radioactive waste from such operations.

Security Organizations. Military law enforcement, military criminal investigative organizations, and DoD contracted security personnel.

Terrorism. The calculated use of unlawful violence or threat of unlawful violence to inculcate fear and intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

Terrorist. An individual who uses unlawful violence, terror, and intimidation to achieve a result in pursuit of political, religious, or ideological objectives.

Terrorist Group. Any element, regardless of size or espoused cause that commits unlawful acts of violence or threatens unlawful violence in pursuit of its political, religious, or ideological objectives.

Terrorist Threat Level. An intelligence threat assessment of the level of terrorist threat faced by U.S. personnel and interests. The assessment is based on a continuous intelligence analysis of a minimum of four elements: terrorist group operational capability, intentions, activity, and operational environment. There are four threat levels: LOW, MODERATE, SIGNIFICANT, and HIGH. Threat levels should not be confused with FPCONs. Threat level assessments are provided to senior leaders to assist them determine the appropriate local FPCON.

Vulnerability. In antiterrorism, a situation or circumstance, if left unchanged, that may result in the loss of life or damage to mission-essential resources. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level

of effects in an unnatural (manmade) hostile environment. In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system.

(This page intentionally left blank)

AT/CIP T&R MANUAL

APPENDIX D

AT CHECKLIST FOR COMMANDERS AND AT OFFICERS

(This appendix is not intended to be doctrinal in nature but rather a tool for Commanders and ATOs to use when building, evaluating, and improving their antiterrorism programs.)

INTRODUCTION. Protection of DoD assets is an inherent obligation of management and military commanders. The following checklist is a self-assessment, management tool that can be used by the commanders, agency manager, and/or unit AT Officer to assess the status of his/her AT program. Not all the standards are applicable to all levels of command; therefore, Combatant Commander and Service AT guidance should be used where applicable.

1. Questions for commanders/managers to evaluate AT program adequacy:

Table T1: Antiterrorism Checklist - Commanders

DoD Std	AT METRIC
4, 6, 14, 22	<u>Assuming Command:</u> Does unit have an AT program and security posture appropriate for mission and potential threat? AT Officer appointed? AT Working Group (ATWG) designated? DIA and/or FBI Threat Assessment current? Vulnerability assessment current? AT Plan complete? Program review within past 12 months? AT Plan exercised within past 12 months? AT Level I training current? Have you reviewed DoDI 2000.16 and appropriate Combatant Commander/Service AT guidance? Is Combatant Commander/Service AT guidance implemented?
4, 5, 14, 24	<u>Organize for AT:</u> Does unit have adequate focus on AT? Is unit ATO school trained? Are right functions represented in ATWG? Is ATWG active? Meeting minutes? Accomplishments? Next meeting? Next action?
4, 7, 8, 9, 10, 15	<u>Threat Assessment:</u> Do Threat Assessments provided by DIA and/or FBI and/or the local threat assessment process? Identify specific terrorist capabilities, weapons, and tactics (to include WMD). Provide the necessary information for the commander to help tailor Force Protection Conditions. Have a review mechanism to provide up to date information. Is unit aware of current and potential threats (conventional and WMD)? DIA and/or FBI (CONUS) assessed threat level for area? Combatant Commander-assigned higher local threat level? Formal Intel assessment on hand & current? Relationship with supporting Intel activity? Is Counter-Intelligence or law enforcement support needed?

DoD Std	AT METRIC
	Local information considered? Local information network established? Aggressive list of threat options identified?
26, 27	<u>Vulnerability Assessment (VA):</u> Do Vulnerability Assessments & the vulnerability process include? The range of terrorist threat identified in the Threat Assessment. Recommendations for procedural enhancements and resource requirements. Provided complete inventory of assets & areas? Prioritization of assets/areas on criticality? Catalog of known vulnerabilities? Provide for annual revisions. Has unit evaluated the vulnerability of all assets to potential threats to support risk management decisions? When was the last Vulnerability Assessment? Did last VA reveal significant vulnerabilities? What is status of remedial actions? Next scheduled VA?
11, 12, 13, 14, 15, 16, 17, 18	<u>Antiterrorism Plan (see Appendix G for AT Plan sample):</u> Does my unit have a suitable AT plan? How is this plan documented? (Five par. order, or annexes to other orders?) Does the plan specify the AT mission and concept of operation? Does the plan layout the task organization and Mission Essential or Vulnerable Areas (MEVAs)? Does the plan include the Risk Management process, to include annual AT Threat Assessment with WMD coverage? Is there a process, based on local terrorism threat information to raise FPCONs? Does plan provide actions at each FPCON? Does plan provide a baseline for normal ops? What FPCON measures have been adopted due to local threat? Does plan provide diagram for Random Antiterrorism Measures (RAMs)? Does the plan include Security Force operations (including augmentation forces) and post priorities? Has plan been reviewed within past year to remediate procedural and resource shortfalls? Has plan been approved by higher HQ? Received/approved AT plans from lower HQ? Is the plan executable? Is the plan resourced? Does plan mitigate vulnerabilities with policy and procedural solutions? Does plan address response to incident and mass casualties? Does the AT plan contain, as a minimum, site specific procedures for? Terrorism Threat Assessments. AT Physical Security Measures. Mass notification procedures. Incident Response Measures. Consequence Management Measures. AT considerations for plans/orders for temporary operations or exercises. Does the command have an adequate "Baseline" security posture to include? General AT and physical security awareness.

DoD Std	AT METRIC
	<p>Adequately equipped and trained First Response Forces.</p> <p>A security posture, capable of sustained operations and commensurate to the local threat that adequately protects personnel and assets.</p> <p>Plans and procedures to transition from Normal Operations to and Elevated state of readiness/execution.</p> <p>Is there a process for you to evaluate subordinate units and/or tenant commands knowledge and status of their AT responsibilities?</p>
19	<p><u>AT Exercises:</u></p> <p>Has AT plan been validated by exercises and is unit ready to execute it?</p> <p>Has AT plan been exercised within one year?</p> <p>Have key organizations exercised their roles?</p> <p>Unit response to increasing threat levels been exercised?</p> <p>Unit response to incident/mass casualties been exercised?</p> <p>AT plan been exercised in a manner to heighten awareness?</p> <p>Incorporated RAMs?</p> <p>Has exercise identified discrepancies? Plan to correct them?</p>
28, 29, 30, 31	<p><u>Antiterrorism Resources:</u></p> <p>Does AT resource program support the required long-term security posture?</p> <p>Defined resource requirements to mitigate security deficiencies?</p> <p>Requirements justified with risk analysis?</p> <p>Alternative plans, policy, and procedural solutions considered or implemented?</p> <p>Does the command have a formal process to track, document, and justify resource requirements and identify resource shortfalls to Higher Headquarters?</p> <p>Higher HQ approved these requirements?</p> <p>Does the command request Combating Terrorism Readiness Initiative Funds for emergent and or emergency Combatant Commander AT requirements?</p> <p>Emergent (OCONUS) needs submitted for immediate support by Combating Terrorism Readiness Initiative Fund (CbT-RIF)?</p> <p>Does the command incorporate AT requirements into the Program Change Proposal process?</p> <p>Are Program Change Proposal requirements submitted for out year support of CbT-RIF funded investments?</p> <p>Status of CbT-RIF and Program Change Proposal requirements in the program/budget process?</p> <p>AT and security factors adequately weighed in acquisition and use of facilities (both temporary and permanent)?</p> <p>Current facilities conform to DoD and Component AT MILCON standards?</p> <p>Do structural engineers and security personnel work together to incorporate AT consideration in building design and review?</p> <p>Are DoD AT Standards for buildings incorporated into new constructions?</p> <p>How is technology being used to enhance security and human performance?</p> <p>What technologies have been identified as recommended/required for higher threat levels/FPCONS?</p> <p>Is the AT Officer a member of the Resource Management Committee?</p>
19, 21, 22,	<p><u>AT Training:</u></p> <p>Are personnel receiving the appropriate levels of AT training to include?</p>

DoD Std	AT METRIC
23, 24, 25	<p>Level I-IV training. High Risk Personnel. AOR specific training prior to deployment. A system to track and document training. Is individual awareness of terrorism threat sufficient for threat environment/mission? Annual Level I training current? AOR updates current and briefed? Special local individual protective measures briefed and used?</p>
5, 14, 20	<p><u>Program Review:</u> Is AT program comprehensive, current, and effective? Can unit do mission under FPCONs in use? Are critical FPCONs compromised for unit morale or convenience? Is AT a routine element of daily mission planning and execution? Are operational patterns varied? Is OPSEC included in mission planning? Does unit continually monitor threat and corresponding security posture? Does unit monitor and control access of visitors and employees in sensitive areas? Has threat level changed since last VA? Is threat assessment current and valid? Are RAMs having desired effect on unit awareness, readiness, and deterrence?</p>
4	<p><u>MoU/MoA:</u> Is unit conforming to and employing MOU/MOA for local support? Does unit or any detached personnel fall under State Department for force protection? Are State Department's force protection instructions on hand for those individuals? Identified organizations with jurisdiction for law enforcement, health, safety, and welfare of assigned service members on and off duty? Unit conforming to jurisdictional agreements in these areas (SOFA, inter-agency)? Identified local community organizations with shared security interests (police, federal law enforcement, hospitals, and public health)? Mutual aid agreements in place with local community to leverage shared interests? Mutual aid agreements been reviewed by higher HQ? Mutual aid agreements executable (liability, jurisdiction, capabilities)?</p>
10, 17, 18	<p><u>Mitigate WMD Effects:</u> Has unit prepared for WMD attack? Does AT plan consider terrorist use of WMD (CBRNE)? What are AT plan assumptions concerning the worst case threat options? Procedures for detection of unconventional CBRNE attacks? Unit training include awareness of indicators of unconventional attacks? Do all personnel have individual protective equipment available? Are collective protective systems available? What NBC detection equipment is available? What decontamination equipment is available?</p>

DoD Std	AT METRIC
28, 29, 30	<u>Off-installation Housing:</u> Are troops housed off-installation adequately secured? Service members in Moderate, Significant, and High threat areas receive instruction and supervision in residential security measures? In such areas, do unit AT response plans include current residence location information for all unit members residing off installation? In such areas, do units coordinate with local law enforcement authorities for protection of unit members residing off-installation (MOUs/MOAs/SOFs)? Incident response plans include measures for off-installation personnel (personnel warning system)?
16, 23	<u>Rules of Engagement (RoE)/Rules of Force (RoF):</u> Does unit have correct RoE/RoF guidance for the mission and environment? Do plan/current procedures provide enough "stand-off" to determine hostile intent and make proper decision to use force? Are troops trained for making ROE/RUF decisions in realistic situations? RoE/threat scenarios adequate & rigorous? Is unit prepared to apply RoE/RoF for threat scenarios?

2. Questions for Facilities ATOs

Table T2: Antiterrorism Checklist - ATOs

DoD Std	AT METRIC
1	DoD AT Policy: This standard does not apply.
2	<u>Development of AT Standards</u> Do you have a copy of the applicable DoD, Combatant Commander, Service, and Agency AT regulations, standards, and other guidance? Combatant Commander/Service and/or DoD Agency Standards should address: Procedures to collect and analyze terrorist threat information, threat capabilities, and vulnerabilities to terrorist attacks. Terrorism threat assessment, Vulnerability Assessment, Terrorism Incident Response Measures, and Terrorist Consequence Management measures. AT Plans and procedures to enhance AT protection. Procedures to identify AT requirements and to program for resources necessary to meet security requirements. DoD Military AT constructions considerations.
3	<u>Assignment of AT Operational Responsibility</u> Does facility understand which Combatant Commander, Service or DoD Agency has AT Tactical Control (TACON) for operational responsibility?
4	<u>AT Coordination in Overseas Locations:</u> This standard does not apply to facility AT Plans.
5	<u>Comprehensive AT Development, Implementation, and Assessment</u> Does the installation AT Program contain, as a minimum, the following elements: Threat Assessments (Standard 15). Planning (Standards 14-20) Exercises (Standard 19)

DoD Std	AT METRIC
	<p>Program Review (Standard 20)</p> <p>Training (Standards 19, 21-25)</p> <p>Vulnerability Assessments (Standards 26-27)</p>
6	<p><u>Antiterrorism Officers (ATO) Assigned in Writing</u></p> <p>Has the commander designated a Level II qualified/trained commissioned officer, non-commissioned officer, or civilian staff officer in writing as the ATO?</p> <p>For deploying organizations (e.g. battalion, squadron, ship) have at least one Level II qualified individual designated in writing?</p> <p>Has the ATO attended a Service approved Level II AT Training course?</p>
7	<p><u>Application of Department of Defense Terrorism Threat Analysis Methodology</u></p> <p>Does the unit use the DoD threat level methodology (<i>Low, Moderate, Significant, High</i>) in their local threat assessments?</p>
8	<p><u>Threat Information Collection and Analysis</u></p> <p>Has the commander tasked the appropriate organization under their command to gather, analyze, and disseminate terrorism threat information?</p> <p>Are personnel in the command encouraged and trained to report information on individuals, events, or situations that could pose a threat to the security of DoD personnel, families, facilities, and resources?</p> <p>Does the command have procedures to receive and process Defense Terrorism Warning Reports and/or higher headquarters threat message?</p>
9	<p><u>Threat Information Flow</u></p> <p>Does the command forward all information pertaining to suspected terrorist threats, or acts of terrorism involving DoD personnel or assets for which they have AT responsibility up and down the chain of command?</p> <p>Does the command ensure there is intelligence sharing between all organizations?</p> <p>Does the command provide tailored threat information for transiting units?</p>
10	<p><u>Potential Threat of Terrorist Use of Weapons of Mass Destruction (WMD)</u></p> <p>Does the command have the procedures to process immediately through the chain of command reports of significant information obtained identifying organizations with WMD capability in their AOR?</p> <p>Is an estimate of terrorist potential use of WMD indicated in the local threat assessment?</p>
11	<p><u>Adjustment of Force Protection Conditions</u></p> <p>Does the command have a process, based on terrorism threat information and/or guidance from higher headquarters, to raise or lower FPCONs?</p>
12	<p><u>FPCON Measures Implementation</u>. This standard does not apply to facility AT Plans.</p>
13	<p><u>FPCON Measures</u></p> <p>Has the command developed site-specific measures or actions for each FPCON which supplement measures/actions enumerated for each FPCON as listed within Appendix A of DoD 2000.12-H (reference (b))?</p> <p>Does the command have procedures to set and transition between FPCONs?</p> <p>Does the command have procedures to establish a LOWER FPCON than Higher Headquarters?</p> <p>Are site-specific AT measures, linked to FPCONs classified as a minimum, CONFIDENTIAL?</p> <p>Site-specific AT measures separated from the AT plan can remain FOR</p>

DoD Std	AT METRIC
	<p>OFFICIAL USE ONLY.</p> <p>Do FPCONs permit sufficient time and space to determine hostile intent IAW standing ROE?</p>
14	<p><u>Comprehensive AT plan</u></p> <p>Does the command have a signed AT Plan?</p> <p>Is the plan site-specific and address the following key elements?</p> <p>Terrorism Threat Assessment (including WMD).</p> <p>Vulnerability Assessment (see Standard 26).</p> <p>Risk Assessment</p> <p>AT Physical Security measures.</p> <p>Terrorism Incident Response measures.</p> <p>Terrorism Consequence Management measures.</p> <p>Does the installation incorporate AT planning into operations orders for temporary operations or exercises?</p>
15	<p><u>Terrorism Threat Assessment</u></p> <p>Does the command have an annually updated terrorism threat assessment?</p> <p>Does the threat assessment consider the following during the assessment process:</p> <p>Capabilities of the terrorist threat.</p> <p>Vulnerability of the facilities.</p> <p>Criticality of the facilities.</p> <p>Is the threat assessment used as the basis and justification for recommendations on AT enhancements, program/budget requests and establishment of FPCONs?</p> <p>Does the command use a risk assessment to integrate threat and vulnerability assessment information in order to make an informed decision to commit resources and/or enact policies and procedures to mitigate the threat or define the risk?</p> <p>Does the risk assessment analyze the following elements?</p> <p>Terrorist Threat.</p> <p>Criticality of the Assets.</p> <p>Vulnerability of facilities, programs, and systems to terrorist threats.</p> <p>The ability to conduct activities to deter terrorist incidents, employ countermeasures, mitigate the effects of a terrorist incident, and recover from a terrorist incident.</p>
16	<p><u>AT Physical Security Measures</u></p> <p>Does the Installation Commander coordinate and integrate subordinate unit physical security plans and measures into the AT plan?</p> <p>Are physical security measures considered, do they support, and are they referenced in the AT plan to ensure an integrated approach to terrorist threats?</p> <p>Do AT physical security measures include provisions for the use of:</p> <p>Physical Structures.</p> <p>Physical Security Equipment.</p> <p>Chemical, Biological, Radiological detection & protection equipment.</p> <p>Security Procedures.</p> <p>Random Antiterrorism Measures (RAM)</p> <p>Response Forces</p> <p>Emergency measures sufficient to achieve the desired level of AT protection and preparedness to respond to terrorist attack.</p> <p>Are RAMs used for both in-place and transiting forces?</p>
17	<p><u>Terrorist Incident Response Measures (first response)</u></p> <p>Has the command prepared installation-wide and/or shipboard terrorist</p>

DoD Std	AT METRIC
	<p>incident response measures which include:</p> <p>Procedures for determining the nature and scope of the terrorist incident and required response.</p> <p>Procedures for coordinating security, fire, and medical First Responders.</p> <p>Steps to reconstitute the installation's ability to perform AT measures</p> <p>In Moderate, Significant, or High terrorist threat level areas, has the command included residential location information for all DoD personnel and their dependents in their Incident Response Measures?</p>
18	<p><u>Terrorist Consequence Management Measures</u></p> <p>Do CM measures provide for appropriate emergency response and disaster planning and/or preparedness to respond to a terrorist attack for the installation and/or base engineering, logistics, medical, mass casualty response, transportation, personnel administration, and local and/or host nation support?</p> <p>Do CM measures include guidelines for pre-deployment and garrison operations, pre-attack procedures, actions during attack, and post-attack actions?</p>
19	<p><u>Training and Exercises</u></p> <p>Has the command conducted field and staff training (annually) to exercise AT plans to include?</p> <p>AT Physical Security measures.</p> <p>Terrorist Incident Response measures.</p> <p>Terrorist Consequence Management measures.</p> <p>Does the command maintain exercise AARs/Lessons Learned and document actions taken to remediate identified shortfalls for at least a year?</p> <p>Does command pre-deployment training include?</p> <p>Credible deterrence/response.</p> <p>Deterrence-specific tactics, techniques, and procedures.</p> <p>Terrorist scenarios and hostile intent decision-making.</p>
20	<p><u>Comprehensive AT Review</u></p> <p>Does the command review own and subordinate AT programs and plans at least annually to facilitate AT program enhancement?</p> <p>Does the command review the AT program when the terrorist threat level changes?</p>
21	<p><u>General Requirements for AT Training</u></p> <p>Does the command ensure all personnel records are updated to reflect AT training IAW DoD Component policy?</p>
22	<p><u>Level I AT Awareness Training</u></p> <p>Does the command conduct Level I training IAW DoD and Combatant Commander/Service/Agency standards?</p> <p>Does the installation ensure Military Service family members traveling beyond CONUS on official business receive Level I training (i.e., PCS move)?</p>
23	<p><u>AOR-Specific Training Requirements for all Department of Defense Personnel</u></p> <p>Does the command ensure all individuals traveling outside CONUS for either permanent or temporary duty complete Level I AT Awareness Training?</p> <p>Has the command provided Combatant Commander approved AOR specific AT protection information to individuals traveling outside CONUS within three months prior to travel?</p> <p>Does the command ensure intra-theater transiting units receive</p>

DoD Std	AT METRIC
	detailed threat information covering travel routes and sites that will be visited by the unit?
24	<u>Level II Antiterrorism Officer (ATO) Training</u> Does the installation and/or each deployed unit have at least one Level II trained ATO assigned? Have 0-5/0-6 commanders received Level III training prior to assumption of command?
25	<u>Training for High-Risk Personnel and High-Risk Billets</u> Has the command identified high-risk billets and high-risk personnel to higher headquarters annually? Have personnel designated as "Personnel at High-Risk to Terrorist Attack" and "Personnel Assigned to High-Risk Billets" received appropriate AT training?
26	<u>Vulnerability Assessments of Installations</u> Has a local vulnerability assessment been conducted within the past year? Did the vulnerability assessment identify vulnerabilities and means to eliminate or mitigation them? Did the vulnerability assessment identify options for enhanced protection of DoD personnel and assets? Does the AT vulnerability assessment assess the following functional areas at a minimum: AT Plans and Programs. Counterintelligence, Law Enforcement, Liaison, and Intelligence Support. AT Physical Security Measures. Vulnerability to a Threat and Terrorist Incident Response Measures. Vulnerability Assessment for Terrorist Use of WMD. Availability of resources to support plans as written. Frequency and extent to which plans have been exercised. Level and adequacy of support from the host nation, local community, and where appropriate, inter-Service and tenant organizations to enhance force protection measures or respond to a terrorist incident. Status of formal and informal agreements to support AT functions. Does the vulnerability assessment team contain expertise in order to meet the intent of providing comprehensive assessments? Is there a process to track and identify vulnerabilities through the chain of command?
27	<u>Pre-Deployment AT Vulnerability Assessment</u> Has a pre-deployment AT vulnerability assessment been conducted for units prior to deployment? Have appropriate AT measures been implemented to reduce risk and vulnerability? Has the command received onboard and/or advance-site assessments prior to and during visits to higher-threat areas of Significant or High Threat Levels or where a geographically specific Terrorism Threat Warning Report is in effect? Has the command requested funds from CbT RIF for emergent AT requirements prior to movement of forces? Has the command explored the use of Commercial-off-the-shelf or Government-off-the-shelf products to meet near-term AT protection requirements?
28	<u>Construction Considerations</u> Do DoD Components adopt and adhere to common criteria and minimum

DoD Std	AT METRIC
	construction (i.e., new construction, renovation, or rehabilitation) standards to mitigate AT vulnerabilities and terrorist attacks?
29	<p><u>Facility and Site Evaluation and/or Selection Criteria</u></p> <p>Has the command developed a prioritized list of AT factors for site selection for facilities, either currently occupied or under consideration for occupancy by DoD personnel? AT factors should include, but not limited to, screening from direct fire weapons, building separation, perimeter standoff, window treatments, protection of entrances and exits, parking lots and roadways, standoff zone delineation, security lighting, external storage areas, mechanical and utility systems.</p> <p>Has the command used these factors to determine if facilities can adequately protect occupants against terrorism attack?</p>
30	<p><u>AT Guidance for Off-Installation Housing</u></p> <p>Does the command have procedures to ensure DoD personnel assigned to Moderate, Significant, and High Terrorism Threat Level areas, who are not provided on-installation or other Government quarters, are furnished guidance on the selection of private residence to mitigate risk of terrorist attack?</p> <p>Does the command have procedures to conduct physical security reviews of off-installation residences for permanently and temporary-duty DoD personnel in Significant or High Threat Level areas?</p> <p>Based on these physical security reviews, does the command have procedures to provide AT recommendations to residents and facility owners?</p> <p>As appropriate, does the command have procedures to recommend to appropriate authorities the construction or lease of housing on an installation or safer area?</p> <p>Does the command have procedures to complete residential security reviews prior to personnel entering into formal contract negotiations for the lease or purchase of off-installation housing in Significant or High Threat areas?</p> <p>Does the command have procedures to include coverage of private residential housing in AT plans where private residential housing must be used in Moderate, Significant, or High Threat Level areas?</p> <p>In Moderate, Significant, or High Threat areas, does the command incorporate family members and dependent vulnerabilities into antiterrorism assessment, mitigation, and reporting tools for:</p> <p>Facilities used by DoD employees and their dependents.</p> <p>Transportation services and routes used by DoD employees and their dependents.</p>
31	<p><u>Executive Protection and High Risk Personnel Security</u></p> <p>Has the command annually reviewed and revalidated the protective services for executives?</p> <p>Has the command taken necessary measures to provide appropriate protective services for designated individuals in high-risk billets and high-risk personnel?</p> <p>Does the command review needs for supplemental security within 30 days of a change in the Terrorism Threat Level?</p>
	<p><u>Miscellaneous Issues</u></p> <p>Does the command have technology to access critical terrorism intelligence e.g., SIPRNET?</p> <p>Has the 0-6 through 0-8 commander been to Level IV training?</p>

AT/CIP T&R MANUAL

APPENDIX E

SUGGESTED VA METHODOLOGIES

(This appendix is not intended to be doctrinal in nature but rather a tool for Commanders and ATOs to use when building, evaluating, and improving their antiterrorism programs.)

INTRODUCTION

1. Facility Commanders are encouraged to use a RA tool that is simple yet has some quantifiable logic to help in decision making. Assessment teams shall use the methodology to determine terrorist options against specific targets and use them as examples of protection strategies. The suggested tools offered below have their strengths and their weaknesses as with all tools, there is a right tool for the job at hand. As an example, CARVER is not specifically tailored for AT assessments, although it can be used. Likewise, MSHARPP is a targeting analysis tool geared more closely to assessing personnel vulnerabilities. Assessment team members should be cognizant of potential gaps when choosing one methodology over another. The use of the Joint Staff CVAMP will assist commanders and ATOs in managing their command's vulnerabilities and associated funding requirements. MSHARPP.

2. The purpose of the MSHARPP matrix is to analyze likely terrorist targets. Consideration is given to the local threat, likely means of attack available to the enemy, and variables affecting the disposition (e.g., "attractiveness" to enemy, potential psychological effect on community, etc.) of potential targets. This document provides an example of how to use MSHARPP.

3. After developing a list of potential targets, use the MSHARPP selection factors to assist in further refining your assessment by associating a weapon/tactic to a potential target to determine the efficiency, effectiveness and plausibility of the method of attack and to identify vulnerabilities related to the target. After the MSHARPP values for each target or component are assigned, the sum of the values indicate the highest value target (for a particular mode of attack) within the limits of the enemy's known capabilities.

a. Mission. Mission focuses mainly on the threat to the situations, activities, capabilities, and resources on an installation that are vulnerable to a terrorist attack. The mission components consist of the equipment, information, facilities, and/or operations or activities that are necessary to accomplish the installation's mission. When assessing points in this area, determine whether or not an attack on mission components shall cause degradation by assessing the Component's:

(1) Importance. Importance measures the value of the area or assets located in the area, considering their function, inherent nature, and monetary value.

(2) Effect. Effect measures the ramifications of a terrorist incident in the area, considering the psychological, economic, sociological, and military impacts.

(3) Recuperability. Recuperability measures the time required for the function occurring at that area to be restored, considering the availability of resources, parts, expertise and manpower, and redundancies.

(4) Mission Criteria Scale. Assess points to the target equipment, information, facilities, and/or operations or activities (scale of 1-5; 5 being worst) in this area based upon the degree of mission degradation if attacked by a terrorist.

(a) ONE - Destroying or disrupting this asset would have no effect on the ability of the installation to accomplish its mission.

(b) TWO - The installation could continue to carry out its mission if this asset were attacked, albeit with some degradation in effectiveness.

(c) THREE - Half of the mission capability remains if the asset were successfully attacked.

(d) FOUR - Ability to carry out a primary mission of the installation would be significantly impaired if this asset were successfully attacked.

(e) FIVE - Installation cannot continue to carry out its mission until the attacked asset is restored.

b. Symbolism. Consider whether the target represents, or is perceived by the enemy to represent, a symbol of a targeted group (e.g., symbolic of U.S. military, Christianity, government, authority, etc.). Assess points in this area based upon the symbolic value of the target to the enemy. Symbolism criteria scale:

(1) High profile, direct symbol of target group or ideology, asset is perceived to be vital to the mission of the installation.

(2) Low profile, direct symbol of target group or ideology.

(3) Low profile and/or obscure symbol of target group or ideology.

c. History. Do terrorist groups have a history of attacking this type of target? While you must consider terrorist trends worldwide, focus on local targeting history and capabilities. Symbolism criteria scale:

(1) Strong history of attacking this type of target.

(2) History of attacking this type of target, but none in the immediate past.

(3) Little to no history of attacking this type of target.

d. Accessibility. A target is accessible when an operational element can reach the target with sufficient personnel and equipment to accomplish its mission. A target can be accessible even if it requires the assistance of knowledgeable insiders. This assessment entails identifying and studying critical paths that the operational element must take to achieve its objectives, and measuring those things that aid or impede access. The enemy must not only be able to reach the target but must also remain there for an

extended period. The four basic stages to consider, when assessing accessibility are:

- (1) Infiltration from the staging base to the target area.
- (2) Movement from the point of entry to the target or objective.
- (3) Movement to the target's critical element.
- (4) Exfiltration.
- (5) Accessibility criteria scale:
 - (a) Easily accessible, standoff weapons can be employed.
 - (b) Inside Perimeter fence, climbing or lowering required.
 - (c) Not accessible or inaccessible without extreme difficulty.

e. Recognizability. A target's recognizability is the degree to which an operational element and/or intelligence collection and reconnaissance asset under varying conditions can recognize it. Weather has an obvious and significant impact on visibility (yours and the enemy's). Rain, snow, and ground fog may obscure observation. Road segments with sparse vegetation and adjacent high ground provide excellent conditions for good observation. Distance, light, and season must be considered. Other factors that influence recognizability include the size and complexity of the target, the existence of distinctive target signatures, the presence of masking or camouflage, and the technical sophistication and training of the enemy. Recognizability criteria scale:

- (1) Target is clearly recognizable under all conditions and from a distance; requires little or no training for recognition.
- (2) Target is easily recognizable at small-arms range and requires a small amount of training for recognition.
- (3) Target is difficult to recognize at night or in bad weather, or might be confused with other targets; requires training for recognition.
- (4) Target cannot be recognized under any conditions—except by experts.

f. Population. Population addressed two factors, quantity of personnel and their demography. Demography asks the question "who are the targets?" Depending on the ideology of the terrorist group(s), being a member of a particular demographic group can make someone (or some group) a more likely target.

- (1) When assessing points in this area, determine whether or not the group (s) have a history of, or are predicted to target:
 - (a) Military personnel.
 - (b) Family members (U.S. citizens in general).

(c) Civilian employees of the U.S. Government (include local nationals).

(d) Senior officers or other high-risk personnel.

(e) Member of an ethnicity (racial, religious, or regionally defined).

(2) Quantity addresses the number of people that would become victims if a particular target were attacked. Going on the assumption the intent of the attack is to kill or injure personnel, it follows that the more densely populated an area/facility is, the more lucrative a target it makes (all other things being equal).

(3) Population criteria scale.

(a) Densely populated; prone to frequent crowds, facility routinely contains substantial numbers of personnel known to be targeted by the enemy and/or the population is comprised of personnel deemed vital to the accomplishment of the installation's mission.

(b) Relatively large numbers of people, but not in close proximity (i.e., spread out and hard to reach in a single attack), contains known target group, but rarely in large concentrations, population has no special segment necessary for mission accomplishment.

(c) Sparsely populated; prone to having small groups or individuals, little target value based on demographics of occupants

g. Proximity. Is the potential target located near other personnel, facilities, or resources that, because of their intrinsic value or "protected" status and a fear of collateral damage, afford it some form of protection? (e.g., near national monuments, protected/religious symbols, etc., that the enemy holds in high regard).

(1) It is important to consider whether the target is in close proximity to other likely targets. Just as the risk of unwanted collateral damage may decrease the chances of attack; a "target-rich" environment may increase the chances of attack.

(2) Proximity criteria scale.

(a) Target is isolated; no chance of unwanted collateral damage to protected symbols or personnel.

(b) Target is in close enough proximity to place protected personnel, facilities, etc., at risk of injury or damage, but not destruction.

(c) Target is in close proximity; serious injury/ damage or death/total destruction of protected personnel/facilities likely. Figure F1 is an example MSHARPP worksheet. Values from 1 to 5 are assigned to each factor based on the associated data for each target. Five represents the highest vulnerability or likelihood of attack and 1 the lowest. Accordingly, the higher the total score, the more vulnerable the target. Because this analysis is highly subjective, some analysts prefer simple "stoplight" charts with red, yellow and green markers representing descending degrees of

vulnerability. The MSHARPP analysis must consider both the present force protection posture and enhanced postures proposed for escalating FPCONs. Specific target vulnerabilities must be combined with exploitable perimeter control vulnerabilities. If access routes are well protected and not deemed exploitable an otherwise vulnerable building becomes a less likely target.

Figure E1. Example of MSHARPP matrix.

TARGET	M	S	H	A	R	P	P	TOTAL	WEAPON
HQ BLDG	5	4	5	1	3	4	1	23	4,000 Truck IED
Barracks B	2	4	5	4	4	4	2	25	220 lb Car IED
Comm Center	5	4	2	3	5	3	1	23	4,000 Truck IED
SF Ops Center	3	3	2	4	4	4	2	22	7.62 (Sniper)
Fuel Storage	4	3	1	5	5	1	3	22	50 lb Satchel Charge
Hanger A	5	5	3	2	5	5	4	29	Mortar
Wpns Storage	5	5	1	1	5	3	1	21	RPG
Elec Transformer	5	2	3	5	5	0	4	24	Grenade

CARVER

a. The CARVER matrix is used by Special Forces and commandos to target enemy infrastructure including public works facilities such as bridges and power plants. It is believed that our enemies - overt and covert - employ a similar method to target our facilities. They all, though, seek soft, unprotected targets.

b. CARVER is a very useful tool for determining that your critical assets might indeed offer an enemy a good or soft target. If you employ the very same CARVER analysis to every asset, it shall yield a good estimate as to the attractiveness of those assets to an enemy. Specifically Commanders shall then know which "targets" require hardening or otherwise increased protection.

c. CARVER is an acronym, with each letter representing the following:

(1) Criticality. The importance of a system, subsystem, complex, or component. A target is critical when its destruction or damage has a significant impact on the output of the targeted system, subsystem, or complex, and at the highest level, on the unit's ability to make war or perform essential functions. Criticality depends on several factors:

(a) How rapidly shall the impact of asset destruction affect the unit's essential functions?

(b) What percentage of output and essential functions is curtailed by asset damage?

(c) Is there an existence of substitutes for the output product or service?

(d) What is the number of assets and their position in the system or complex flow diagram?

(e) Criticality asks the question: How critical is the facility to your mission accomplishment?

(2) Accessibility. The ease that an asset can be reached, either physically or by standoff weapons. An asset is accessible when a terrorist element can physically infiltrate the asset, or the asset can be hit by direct or indirect fire. As a reminder, assets can be people, places, or things. The use of standoff weapons should always be considered when evaluating accessibility. Survivability of the attacker is usually most related to a target's accessibility. Accessibility asks the question: How easily can an enemy get access to, or have their weapons reach the asset?

(3) Recuperability. A measure of time required to replace, repair or bypass, the destruction or damage inflicted on the target. Recuperability varies with the sources and ages of targeted components and with the availability of spare parts. The existence of economic embargoes and the technical resources of the installation shall influence recuperability. Recuperability asks the question: How long would it take you to repair or replace the asset?

(4) Vulnerability. A measure of the ability of the terrorist to damage the target using available assets (people and material). A target (asset) is vulnerable if the terrorist has the means and expertise to successfully attack it. Vulnerability depends on:

(a) The nature of the construction of the target.

(b) The assets available (manpower, transportation, weapons, explosives, and equipment) to defend the facility.

(c) Vulnerability asks the question: Is the asset literally hardened or guarded? Are measures in place to mitigate any threat?

(5) Effect on the population. The positive or negative influence on the population as a result of the action taken. Effect considers public relation in the vicinity of the target, but also considers the domestic and international reaction as well. Shall reprisals against friendlies result? Shall national PSYOP themes be contradicted or reinforced? Shall exfiltration and evasion be helped or hurt? Shall the enemy population be alienated from its government, or shall it become supportive of the government. Effect is often neutral at the tactical level. Effect asks the question: What is the effect on the local population, be it terror or demoralization, and associated mission degradation?

(6) Recognizability. The degree that a target can be recognized under varying weather, light, and seasonal conditions without confusion with other targets or components.

(a) Factors that influence recognizability include the size and complexity of the target, the existence of distinctive target signatures, and the technical sophistication and training of the terrorists.

(b) Recognizability asks the question: Can the enemy recognize the target for what it truly is and its importance?

d. Target selection requires detailed intelligence and thorough planning, and is based on the CARVER factors identified above. The CARVER

Matrix, as shown in Table T1, is a decision tool for rating the relative desirability of potential targets and for wisely allocating attack resources. Two rules of thumb apply for completing the matrix:

- (1) For strategic level analysis, list systems and subsystems.
- (2) For tactical level analysis list complexes or components of subsystems and complexes. Keep in mind that the scale can be adjusted, such as one to ten or 10 to 100, provided that consistency is observed.

Table T1: Example CARVER Matrix

Potential Targets	C	A	R	V	E	R	TOTAL
Commissary	5	7	10	7	8	10	47

CARVER CRITERIA

Criticality:	Rating
Immediate Output halt or 100% curtailment	10
Output halt less than one day or 75% curtailment	6
Output halt less than one week or 50% curtailment	4
Output halt in over one week and less than 25% curtailment	1
Accessibility:	
Standoff weapons can be deployed	10
Inside perimeter fence, but outdoors	8
Inside of a building, but ground floor	6
Inside of a building, but second floor	4
Inside of a building, climbing required	1
Recuperability:	
One month or more	10
Up to one month	8

Up to one week	6
Up to one day	4
4 hours or less	1
Vulnerability:	
To small arms fire or charges 5 pounds or less	10
To anti-tank weapons or charges of 5 to 10 pounds	7
To charges of 10 to 30 pounds	5
To charges of 30 to 50 pounds	3
More drastic measures must be employed.	1
Effect on the Population:	
National PSYOP objectives fostered; no reprisals against friendlies likely.	10
No effect, or neutral	5
Very negative public reaction, reprisals against friendlies likely, or high domestic uprising potential.	1
Note: On the tactical level, effect on population is often neutral. That is, the effect is the same for all components within a complex. There are conspicuous exceptions, such as reactor components in nuclear sites. If all components within a complex are neutral, the entire "E" column can be removed from the matrix.	
Recognizability:	
The complex or component is recognizable day or night, rain or shine, without confusion with other complexes or components.	10
The complex or component may be difficult to recognize at night or in bad weather or might be confused with other complexes and components.	5

The complex or component is difficult to recognize under any condition and is easily confused with other complexes and components.	1
--	---

After completing the matrix for all assets, total the scores in the right hand column and then rank order those totals to prioritize vulnerabilities.

e. The following are basic mitigation tips to address four of the six CARVER Components:

(1) Reduce criticality. As practicable have a back-up device, system or tested plan to afford mission accomplishment without the asset; create redundancy either physically or operationally; have a tested and viable Continuity Of Operations Plan; and have a fall-back site for conducting the same mission from another location.

(2) Reduce accessibility. Reduce access both, physical and cyber, as applicable; use barriers, other barricades, carefully controlled pedestrian and vehicle movement and/or access and parking; and use fences, remote motion sensors, and remote video surveillance.

(3) Reduce vulnerability. Harden the structure and/or immediate environment to include window treatment to prevent glass shards, structural reinforcement, and shatterproof and fireproof building materials. Move vehicle parking and access sufficiently away from personnel-massing facilities.

(4) Reduce recognizability. Delete location and purpose of facility from all base maps and remove building signs that describe function or give title of unit in facility. Instruct telephone operators to not give out number or existence of facility. Use plant cover, including trees and bushes, to partially conceal facility, particularly from roads.

CORE VULNERABILITY ASSESSMENT MANAGEMENT PROGRAM.

a. CVAMP is an automated and web-based means of managing a command's vulnerabilities and associated funding requirements. CVAMP key capabilities include:

(1) Provide a means to database vulnerability assessment findings in accordance with reference (e), for both higher headquarters and local assessments.

(2) Provide capability of receiving observations directly from the JSIVA Information System.

(3) Document a commander's risk assessment decision for each vulnerability.

(4) Track the status of known vulnerabilities until mitigated.

(5) Provide a tool to assist in prioritizing vulnerabilities via a weighted scale based on user input.

(6) Provide commanders a vehicle to identify requirements to the responsible chain of command.

(7) Provide the ability to roll vulnerability data into a resource requirement. This includes UFR submissions as well as emergent and emergency CbT RIF requests. Use of CVAMP is mandatory for submission to the Joint Staff of CbT RIF requests.

(8) Provide ability to control release of vulnerabilities and associated funding requests through the chain of command - access is limited to a "need to know" basis as determined by system administrators at each command level.

(9) Allow for prioritization of emergent CbT RIF requests and UFRs as well as provide a tool to assist in this process based on user input.

(10) Provides a ready reference to track the status of installations and activities by FPCON and/or Terrorism Threat Level.

b. Registration for CVAMP is embedded within the Joint Staff's Antiterrorism Enterprise Portal (ATEP) via the SIPRNET. Once registered on ATEP, system administrators identified at each level of command will assign CVAMP roles and functions to users based on their needs/requirements. To allow for flexibility, administrators can assign multiple roles to a user. Each role sets specific user permissions within the system. Besides SIPRNET access, minimal additional equipment or training is required to use CVAMP. The system operates in a user-friendly format with drop down menus and no complex computer skills are required to create, review, modify or manage the program. Initial CVAMP-related roles and their permissions are:

(1) Commander: Capability to read/write with comment and retains sole release authority to higher headquarters on all vulnerability assessments, vulnerabilities, and funding requests.

(2) ATO: Capability to create vulnerability assessments, vulnerabilities and funding requests.

(3) Resource Manager: Capability to read/write to all funding requests.

(4) Assessor: Capability to create observations associated with a vulnerability assessment.

(5) System Administrator: Capability to assign and manage roles within immediate organization and one level down.

(6) Users should contact their local/and or next higher headquarters CVAMP administrators to establish their roles within CVAMP.

AT/CIP T&R MANUAL

APPENDIX F

DOD FPCON SYSTEM (from DoD 2000.12H)

1. BASIC FPCON PROCEDURES

a. General

(1) The FPCONs outlined below describe the progressive level of countermeasures in response to a terrorist threat to U.S. military facilities and personnel as directed by reference (a). These security measures are approved by the Joint Chiefs of Staff and are designed to facilitate inter-Service coordination and support of U.S. Military antiterrorism activities. When installations adapt these measures for their site-specific circumstances, they should account for, as a minimum, Combatant Commander/Service requirements, local laws, and SOFA. Per reference (e), FPCONs measures are FOR OFFICIAL USE ONLY. An AT Plan with a complete listing of site-specific AT measures, linked to a FPCON, will be classified, as a minimum, CONFIDENTIAL. When separated from the AT Plan, specific measures and FPCON measures remain FOR OFFICIAL USE ONLY.

(2) Once a FPCON is declared, all listed security measures are implemented immediately unless waived by competent authority as described in Chapter 10. The declared FPCON should also be supplemented by a system of RAMs in order to complicate a terrorist group's operational planning and targeting.

(3) Airfield specific measures are for installations and facilities with a permanently functioning airfield. Installations and facilities with an emergency helicopter pad should review and implement any applicable airfield specific measures when they anticipate air operations.

(4) Due to their specific security requirements, DoD ship's measures are listed separately. Those measures applying solely to USN combatant ships are further identified throughout the paragraph. Shipboard guidelines are specially tailored to assist commanding officers and ship masters in reducing the effect of terrorist and other security threats to DoD combatant and non-combatant vessels, to include U.S. Army and Military Sealift ships worldwide. They provide direction to maximize security for the ship based on current threat conditions consistent with performance of assigned missions and routine functions.

(5) Specific countermeasures were determined taking into consideration the following factors:

(a) Ability to maintain highest state of operational readiness.

(b) Measures to improve physical security through the use of duty and guard force personnel limit access to the exposed perimeter areas and interior of the unit/facility by hostile persons, and barriers to physically protect the unit/facility.

(c) Availability of effective command, control, and communication systems with emphasis on supporting duty/watch officers, security forces, and key personnel.

(d) An AT awareness program for all personnel.

(e) Protection of high-risk assets and personnel.

(f) Measures necessary to limit activities, and visitor/social engagements.

b. FPCON NORMAL and all FPCON levels should include site-specific measures a facility commander deems necessary when establishing a baseline posture.

2. FPCON NORMAL

a. Measure NORMAL 1. Secure and randomly inspect buildings, rooms, and storage areas not in regular use.

b. Measure NORMAL 2. Conduct random security spot checks of vehicles and persons entering facilities under the jurisdiction of the United States.

c. Measure NORMAL 3. Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.

3. FPCON ALPHA MEASURES

a. Measure ALPHA 1. Continue, or introduce, all measures in previous FPCON.

b. Measure ALPHA 2. At regular intervals, inform personnel and family members of the general situation. Ensure personnel arriving for duty are briefed on the threat. Also, remind them to be alert for and report suspicious activities, such as the presence of unfamiliar personnel and vehicles, suspicious parcels, and possible surveillance attempts.

c. Measure ALPHA 3. The duty officer or personnel with access to building plans as well as the plans for area evacuations must be available at all times. Plans should be in place to execute access control procedures. Key personnel required to implement security plans should be on-call and readily available.

d. Measure ALPHA 4. Increase security spot checks of vehicles and persons entering installations under the jurisdiction of the United States.

e. Measure ALPHA 5. Initiate food and water Operational Risk Management (ORM) procedures, brief personnel on food and water security procedures, and report any unusual activities.

f. Measure ALPHA 6. Test mass notification system.

g. Measure ALPHA 7. Review all plans, identify resource requirements, and be prepared to implement higher FPCONs.

h. Measure ALPHA 8. Review and, if necessary, implement security measures for high-risk personnel.

i. Measure ALPHA 9. As appropriate, consult local authorities on the threat and mutual antiterrorism measures.

j. Measure ALPHA 10. Review intelligence, counter intelligence, and operations dissemination procedures.

4. FPCON BRAVO MEASURES

a. Measure BRAVO 1. Continue, or introduce, all measures in previous FPCONs.

b. Measure BRAVO 2. Enforce control of entry onto U.S. infrastructure critical to mission accomplishment, lucrative targets, and high profile locations; and randomly search vehicles entering these areas. Particular scrutiny should be given to vehicles that are capable of concealing a large IED (cargo vans, delivery vehicles) sufficient to cause catastrophic damage or loss of life.

c. Measure BRAVO 3. Identify critical and high occupancy buildings. Keep cars and objects (e.g., crates, trash containers) away from buildings to reduce vulnerability to bomb attacks. Apply this criterion to all inhabited structures to the greatest extent possible. Standoff distance should be determined by the following factors: asset criticality; the protection level provided by structure, IED/Vehicle Borne IED (VBIED) threat; and available security measures. Consider centralized parking.

d. Measure BRAVO 4. Secure and inspect all buildings, rooms, and storage areas not in regular use.

e. Measure BRAVO 5. At the beginning and end of each workday, as well as at random intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.

f. Measure BRAVO 6. Implement mail-screening procedures to identify suspicious letters and parcels.

g. Measure BRAVO 7. Randomly inspect commercial deliveries. Advise family members to check home deliveries.

h. Measure BRAVO 8. Randomly inspect food and water for evidence of tampering/contamination before use by DoD personnel. Inspections should include delivery vehicles and storage area/containers.

i. Measure BRAVO 9. Increase security/guard presence or patrol/surveillance of DoD housing areas, schools, messes, on-base clubs, and similar high-occupancy targets to improve deterrence and defense, and to build confidence among staff and family members.

j. Measure BRAVO 10. Implement plans to enhance off-installation security of DoD facilities. In areas with Threat Levels of Moderate, Significant, or High, coverage includes facilities (e.g., DoD schools and daycare centers) and transportation services and routes (e.g., bus routes) used by DoD employees and family members.

k. Measure BRAVO 11. Inform local security committees of actions being taken.

l. Measure BRAVO 12. Verify identity of visitors and randomly inspect their suitcases, parcels, and other containers.

m. Measure BRAVO 13. Conduct random patrols to check vehicles, people, and buildings.

n. Measure BRAVO 14. As necessary, implement additional security measures for high-risk personnel.

o. Measure BRAVO 15. Place personnel required for implementing AT plans on call; commanders should exercise discretion in approving absences.

p. Measure BRAVO 16. Identify and brief personnel who may augment guard forces. Review specific rules of engagement including the use of deadly force.

q. Measure BRAVO 17. As deemed appropriate, verify identity of personnel entering buildings.

r. Measure BRAVO 18. Review status and adjust as appropriate OPSEC, COMSEC, and INFOSEC procedures.

s. Measure BRAVO 19. (airfield specific) As appropriate, erect barriers and man and establish checkpoints at entrances to airfields. Ensure identity of all individuals entering the airfield (flightline and support facilities) -- no exceptions. Randomly inspect vehicles, briefcases and packages entering the airfield.

t. Measure BRAVO 20. (airfield specific) Coordinate plans to safeguard aircraft departure and approach flight paths with local authorities. Be prepared to activate contingency plans and issue detailed air traffic control procedures. As appropriate, take actions to mitigate threat of surface-to-air missiles or standoff weapons that can be delivered from beyond the airfield perimeter.

5. FPCON CHARLIE MEASURES

a. Measure CHARLIE 1. Continue, or introduce, all measures in previous FPCON.

b. Measure CHARLIE 2. Recall additional required personnel. Ensure armed augmentation security personnel are aware of current ROEs and SOFAs. Review types of weapons and ammunition issued to augmentation security personnel; heightened threats may require employment of different weapons capabilities.

c. Measure CHARLIE 3. Be prepared to react to requests for assistance, from both local authorities and other installations in the region.

d. Measure CHARLIE 4. Limit access points to strictly enforce entry. Randomly search vehicles.

e. Measure CHARLIE 5. Ensure or verify identity of all individuals entering food and water storage and distribution centers, use sign in/out logs at access control/entry points, and limit and/or inspect all personal items.

f. Measure CHARLIE 6. Initiate contingency monitoring for biological and chemical agents as required. Suspend contractors/off-facility users from tapping into facility water system (alternate locally developed measure should be executed when contractors are responsible for DoD water supplies or when water is provided by local (non-DoD) sources or agencies).

g. Measure CHARLIE 7. Increase standoff from sensitive buildings based on threat. Implement barrier plan to hinder vehicle borne attack.

h. Measure CHARLIE 8. Increase patrolling of the facility to include waterside perimeters, if appropriate. Be prepared to assist local authorities in searching for threatening actions/persons outside the facility perimeter. For airfields, patrol or provide observation of approach and departure flight corridors as appropriate to the threat (coordinate with TSA, Marine Patrol, U.S.C.G., and local law enforcement as required to cover off-facility approach and departure flight corridors).

i. Measure CHARLIE 9. Protect all designated infrastructure critical to mission accomplishment. Give special attention to and coordinate with local authorities regarding infrastructure outside the military establishment.

j. Measure CHARLIE 10. To reduce vulnerability to attack, consult local authorities about closing public (and military) roads and facilities and coordinate any other precautionary measures taken outside the installation perimeter.

k. Measure CHARLIE 11. Consider searching suitcases, briefcases, packages, etc., being brought onto the installation through access control points and consider randomly searching suitcases, briefcases, packages, etc., leaving.

l. Measure CHARLIE 12. Review personnel policy procedures to determine course of action for family members.

m. Measure CHARLIE 13. Review access procedures for all non-U.S. personnel and adjust as appropriate. For airfields, consider terminating visitor access to the flightline and support facilities.

n. Measure CHARLIE 14. Consider escorting children to and from DoD schools (among options to consider are escorting school buses, recommending parents escort children to/from school, etc.).

o. Measure CHARLIE 15. (airfield specific) Reduce flying to essential operational flights only. Implement appropriate flying countermeasures as directed by the Flight Wing Commander (military aircraft) or TSA (civilian aircraft). Consider relief landing ground actions to take for aircraft diversions into and out of an attacked airfield. Consider augmenting fire-fighting details.

6. FPCON DELTA MEASURES

a. Measure DELTA 1. Continue, or introduce, all measures in previous FPCON.

b. Measure DELTA 2. Augment guards as necessary.

c. Measure DELTA 3. Identify all vehicles within operational or mission support areas.

d. Measure DELTA 4. Search all vehicles and their contents before allowing entrance to the installation. Selected pre-screened and constantly secured vehicles used to transport escorted very important personnel are exempted.

e. Measure DELTA 5. Control facility access and implement positive identification of all personnel--no exceptions.

f. Measure DELTA 6. Search all suitcases, briefcases, packages, etc., brought into the installation.

g. Measure DELTA 7. Close DoD schools and/or escort children to/from DoD schools as required.

h. Measure DELTA 8. Make frequent checks of the exterior of buildings and of parking areas.

i. Measure DELTA 9. Restrict all non-essential movement.

j. Measure DELTA 10. (airfield specific) Cease all flying except for specifically authorized operational sorties. Be prepared to deploy light aircraft and/or helicopters for surveillance tasks or to move internal security forces. Implement, if necessary, appropriate flying countermeasures.

k. Measure DELTA 11. (airfield specific) As appropriate, airfields should prepare to accept aircraft diverted from other stations.

l. Measure DELTA 12. If permitted, close public and military roads and facilities. If applicable, close military roads allowing access to the airfield.

7. SHIPBOARD FPCON MEASURES

a. General

(1) The measures outlined below do not account for local conditions, regulations, special evolutions, or current threat intelligence. The command must maintain flexibility. As threat levels or assessments change, the ship's crew must be prepared to take actions to counter the threat. When necessary, additional measures must be taken immediately. While the simple solution to FPCON CHARLIE or DELTA is to get underway, this option may not always be available.

(2) Prior to a ship pulling into any port outside of its homeport, the ship shall have an in-port force protection plan approved by the appropriate Commander. Measures to be taken shall be consistent with local rules, regulations, SOFA and the approved in-port force protection plan.

(3) The duty of the security watch is to safeguard the ship and the ship's company from sabotage, terrorism, civil disturbance, danger, or compromise. The Officer of the Deck (OOD) or equivalent is directly responsible to the Command Duty Officer (CDO) or equivalent, for posting all security watches/sentries and shall ascertain that personnel on watch are

familiar with and proficient in their duties. All watch standers bearing arms shall be properly qualified.

(4) Shipboard FPCON measures are designed to protect vessels in port or at anchorage.

b. General Physical Security Procedures for afloat units:

(1) Anyone with reason to believe the ship is in danger of sabotage or terrorist attack shall immediately notify the Officer of the Day.

c. All hands shall be alert for attempts to board the ship at locations other than the bows, sea ladders, or normal access areas.

(1) Where hostile or subversive elements exist, all hands shall be alert for floating mines or attempts to attach limpet mines to the ship.

(2) Any person who desires to visit the ship shall be denied access until cleared by the OOD.

(3) Material brought aboard shall be randomly inspected by watchstanders, designated members of the Master-at-Arms force, or other petty officers trained in proper inspection procedures. When practical, these inspections shall be conducted prior to bringing material aboard. Contract tools/materials or ship's stores/equipment and like items are to be inspected as soon as practical on weather decks or hangar decks before being struck below.

d. Pre-Port procedures. High levels of activity (aboard ship and on the pier when a vessel arrives in port) must not be allowed to degrade security. Security must be integrated into pre-arrival procedures and should include the following actions:

(1) Obtain a current threat assessment from the local NCIS representative.

(2) The appropriate senior commander shall issue security requirements for all ships.

(3) Brief crew on threat, security precautions, recall procedures, and ship's Self Defense Force (SDF) duties.

(4) Muster security forces, brief threat specifics, review rules of engagement or use of force policies, security assignments, and responsibilities.

(5) Brief beach guards and shore patrols on threats and review special procedures applicable to the specific port visit including pier and/or fleet landing security and access control procedures.

(6) When operating under FPCON BRAVO, in non-Navy ports, or a threat to a specific ship is received use, a Military Working Dog and divers to conduct a search of the pier prior to the ship's arrival when available.

(7) If a suspicious item is found, notify the appropriate Explosive Ordnance Disposal unit. Once cleared, shore security elements shall maintain security until relieved by ship's personnel.

(8) FPCON NORMAL should include ship specific measures a Commander deems necessary when establishing a baseline posture.

8. FPCON NORMAL

a. Measure NORMAL 1. Brief crew on the port specific threat, the security/AT plan, and security precautions to be taken while ashore. Ensure all hands are knowledgeable of various FPCON requirements and that they understand their role in implementation of measures.

b. Measure NORMAL 2. Remind all personnel to be suspicious and inquisitive of strangers, be alert for abandoned parcels or suitcases and for unattended vehicles in the vicinity. Report unusual activities to the OOD, Master or Mate on watch, as applicable.

c. Measure NORMAL 3. Secure and periodically inspect spaces not in use.

d. Measure NORMAL 4. Review security plans and keep them available.

e. Measure NORMAL 5. Review pier and shipboard access control procedures including land and water barriers.

f. Measure NORMAL 6. Ensure sentries/Mate on Watch, roving patrols and the quarterdeck/gangway watch have the ability to communicate with one another.

g. Measure NORMAL 7. Coordinate pier/fleet landing security requirements with SOPA, collocated forces, and/or husbanding agent. Identify anticipated needs for mutual support and define methods of implementation and communication.

9. FPCON ALPHA MEASURES

a. Measure ALPHA 1. Muster, arm, and brief security personnel on the threat and rules of engagement. Keep key personnel who may be needed to implement security measures on call.

b. Measure ALPHA 2. USN combatant ships when in a non-U.S. Navy controlled port, deploy barriers to keep vehicles away from the ship if possible (100 feet in U.S. ports and 400 feet outside U.S. (minimum standoff distances). DoD non-combatants in a non-U.S. Government controlled port, request husband agent arrange and deploy barriers to keep vehicles away from the ship if possible (100 feet in U.S. ports and 400 feet outside U.S. (minimum standoff distances).

c. Measure ALPHA 3. (USN combatant ship specific) Randomly inspect vehicles entering pier.

d. Measure ALPHA 4. Randomly inspect hand carried items and packages before they are brought aboard.

e. Measure ALPHA 5. Regulate shipboard lighting to best meet the threat environment.

f. Measure ALPHA 6. When in a non-U.S. Government controlled port, rig hawsepipe covers and rat guards on lines, cables and hoses. Consider using an anchor collar.

g. Measure ALPHA 7. When in a non-U.S. Government controlled port, raise accommodation ladders, stern gates, ladders, etc when not in use.

h. Measure ALPHA 8. Increase frequency of security drills.

i. Measure ALPHA 9. Establish internal and external communications; including connectivity checks with local operational commander/agencies/authorities that shall be expected to provide support, if required.

10. FPCON BRAVO MEASURES

a. Measure BRAVO 1. Continue or introduce all measures in previous FPCON.

b. Measure BRAVO 2. Set Material Condition YOKE (secure all watertight door and hatches), main deck and below.

c. Measure BRAVO 3. Consistent with local rules, regulations, and/or the SOFA: USN combatant ships post armed pier sentries as necessary; and non-combatant ships post pier sentries (armed at the Master's discretion) as necessary.

d. Measure BRAVO 4. Restrict vehicle access to the pier. Discontinue parking on the pier. Consistent with local rules, regulations, and/or the SOFA, establish unloading zones and move all containers as far away from the ship as possible (recommend 100 feet in the United States, 400 feet outside the United States as the minimum stand-off distance).

e. Measure BRAVO 5. Consistent with the local rules, regulations, and/or the SOFA: USN combatant ships post additional armed watches as necessary; and non-combatant ships post additional watches (armed at the Master's discretion) as necessary. Local threat, environment and fields of fire should be considered when selecting weapons.

f. Measure BRAVO 6. Post signs in local language specifying visiting and loitering restrictions clearly.

g. Measure BRAVO 7. When in a non-U.S. Government controlled port, identify and randomly inspect authorized watercraft, such as workboats, ferries and commercially rented liberty launches, daily.

h. Measure BRAVO 8. When in a non-U.S. Government controlled port, direct liberty boats to make a security tour around the ship upon departing from and arriving at the ship, with particular focus on the waterline and under pilings when berthed at a pier.

i. Measure BRAVO 9. Inspect all visitors' hand carried items, and packages before allowing them aboard. Where available, use baggage scanners and walk through or hand held metal detectors to screen visitors and their packages prior to boarding the ship.

j. Measure BRAVO 10. Implement measures to keep unauthorized craft away from the ship. Authorized craft should be carefully controlled. Coordinate with host nation's husbanding agent/local port authority, as necessary, and request their assistance in controlling unauthorized craft.

k. Measure BRAVO 11. Raise accommodation ladders, etc, when not in use. Clear ship of all unnecessary stages, camels, barges, oil donuts, and lines.

l. Measure BRAVO 12. Review liberty policy in light of the threat and revise it, as necessary to maintain safety and security of ship and crew.

m. Measure BRAVO 13. USN combatant ships conduct division quarters at foul weather parade. All DoD ships avoid conducting activities that shall gather large number of crewmembers at the weatherdecks. Where possible, relocate such activities inside the skin of the ship.

n. Measure BRAVO 14. Ensure an up-to-date list of bilingual personnel for area of operations is readily available. Maintain warning tape, in both the local language and English, is in bridge/pilot house/quarterdeck, for use on the ship's announcing system to warn small craft to remain clear.

o. Measure BRAVO 15. If not already armed, arm the quarterdeck/gangway or mate on watch.

p. Measure BRAVO 16. If not already armed, consider arming the sounding and security patrol.

q. Measure BRAVO 17. Review procedures for expedient issue of firearms and ammunition to the shipboard self-defense force (SSDF)/reaction force and other members of the crew, as deemed necessary by the commanding officer/master.

r. Measure BRAVO 18. Instruct watches to conduct frequent, random searches of pier to include pilings and access points.

s. Measure BRAVO 19. Conduct visual inspections of the ship's hull and ship's boats at intermittent intervals and immediately before it is put to sea using both landside personnel and waterside patrols.

t. Measure BRAVO 20. Hoist ships boats aboard when not in use.

u. Measure BRAVO 21. Terminate all public visits. In U.S. Government controlled ports, host visits (family, friends, small groups sponsored by the ship) may continue at the commanding officer's/master's discretion.

v. Measure BRAVO 22. After working hours, reduce entry points to ship's interior by securing infrequently used entrances. Safety requirements must be considered.

w. Measure BRAVO 23. In non-U.S. Government controlled ports, use only one brow/gangway to access ship (remove any excess brows/gangways). CV(N)s and other large decks may use two as required, when included in an approved AT Plan specific to that port visit.

x. Measure BRAVO 24. In non-U.S. Government controlled ports, maintain capability to get underway on short notice or as specified by standard operating procedures.

y. Measure BRAVO 25. In non-U.S. Government controlled ports, consider layout of fire hoses. Brief designated crew personnel on procedures for repelling boards, small boats and ultra-light aircraft.

z. Measure BRAVO 27. Where possible, monitor local communications (ship to ship, TV, radio, police scanners, etc).

aa. Measure BRAVO 28. As appropriate, inform local authorities of actions being taken as FPCON increases.

bb. Measure BRAVO 29. (USN combatant ship specific) If the threat situation warrants, deploy picket boats to conduct patrols in the immediate vicinity of the ship. Brief boat crews and arm with appropriate weapons considering threat, the local environment, and fields of fire.

11. FPCON CHARLIE MEASURES

a. Measure CHARLIE 1. Continue or introduce all measures in previous FPCON.

b. Measure CHARLIE 2. Consider setting Material Condition Zebra (secure all access doors and hatches), main deck and below.

c. Measure CHARLIE 3. Cancel liberty. Execute emergency recall.

d. Measure CHARLIE 4. Prepare to get underway on short notice. If conditions warrant, request permission to sortie/get underway.

e. Measure CHARLIE 5. Block unnecessary vehicle access to the pier.

f. Measure CHARLIE 6. Coordinate with host nation husbanding agent and/or local port authorities to establish small boat exclusion zone around ship.

g. Measure CHARLIE 7. (USN combatant ship specific) Deploy the SSDF to protect command structure and augment posted watches. Station the SSDF in positions that provide 360 degrees coverage of the ship.

h. Measure CHARLIE 8. Energize radar and or sonar, rotate screws and cycle ruder(s) at frequent and irregular intervals, as needed to assist in deterring, detecting or thwarting attacks.

i. Measure CHARLIE 9. Consider manning repair locker(s). Be prepared to man one repair locker on short notice. Ensure adequate lines of communications are established with damage control central.

j. Measure CHARLIE 10. (USN combatant ship specific) If available and feasible, consider use of airborne assets as an observation/force protection platform.

k. Measure CHARLIE 11. If a threat of swimmer attack exists, activate an anti-swimmer watch.

l. Measure CHARLIE 12. In non-U.S. Government controlled ports and if unable to get underway, consider requesting armed security augmentation from area Combatant Commander.

12. FPCON DELTA MEASURES

- a. Measure DELTA 1. Continue or introduce all measures in previous FPCON.
- b. Measure DELTA 2. Permit only necessary personnel topside.
- c. Measure DELTA 3. If possible, cancel port visit and get underway.
- d. Measure DELTA 4. Employ all necessary weaponry to defend against attack.

AT/CIP T&R MANUAL

APPENDIX G

SAMPLE INSTALLATION ANTITERRORISM PLAN FORMAT
(from MCO 3302.1D)

1. OVERVIEW

a. The format outlined below is offered as one means of developing an AT plan. It is optimized for a base or installation, but can be adapted for other facilities and deployed units. It is meant to help the AT officer structure the AT plan in a comprehensive and organized manner. The format is patterned after the standard five-paragraph military operations order (Situation, Mission, Execution, Administration and Logistics, Command and Signal).

b. This format enables the synchronization of existing programs such as Law Enforcement, Physical Security, AT, OPSEC, INFOSEC, High-Risk Personnel protection and other installation efforts. AT Plans should be integrated into all plans and separate annexes. Remember that staff interaction is a crucial element of developing a realistic, executable plan.

c. Although this sample is patterned after the military operations order, it is applicable to managers of OSD Agencies as they develop plans to protect personnel, activities, and material under their control.

d. This sample uses supporting Annexes, Appendices, Tabs, and Enclosures to provide amplifying instructions as required. This method shortens the length of the basic plan (which should be read by all personnel outlined in the plan), and provides organization, structure, and scalability.

Copy no. ____ of ____ Copies

Installation/Operation Name

Location

Date/Time Group

INSTALLATION/OPERATION NAME ANTITERRORISM PLAN 2004 (AT-04)

Task Organization. Include all agencies/personnel (base and civilian) responsible to implement the plan. Include as a separate Annex. See Annex A (Task Organization).

Maps/Charts: List all applicable maps or charts. Include enough data to ensure personnel are using the correct year/edition/version of the subject material.

Time Zone: Enter the time zone of the installation. Indicate the number of hours to calculate (plus/minus) ZULU time.

Ref: Enter the compilation of pertinent publications, references, MOU/MOA/MAA. This list may be included in a separate Annex. See Annex Q (References).

1. SITUATION

a. General. This plan applies to all personnel assigned or attached to the installation. Describe the political/military environment in sufficient detail for subordinate commanders, staffs, and units to understand their role in the installation AT operations.

b. Enemy. The enemy is any adversary capable of threatening the installation's personnel, facilities, and equipment. ENTER the general threat of terrorism to this installation including the intentions and capabilities, identification, composition, disposition, location, and estimated strengths of hostile forces. Include the general threat of terrorist use of WMD against this installation. This information should remain unclassified when possible. See paragraph 1f, Intelligence, on identifying specific threats. This information may be included as a separate Annex. See Annex B (Intelligence).

c. Friendly. ENTER the forces available (both military and civilian) to respond to a terrorist WMD attack. Include the next higher headquarters and adjacent installations, and any units/organizations that are not under installation command, but may be required to respond to such an incident. These units/organizations may include Host Nation (HN) and US military police forces, fire and emergency services, medical, and federal/state and local agencies, special operations forces, engineers, detection (radiological, nuclear, biological, and chemical) decontamination or smoke units, and explosive ordnance disposal (EOD). Include MOAs/MOUs and any other special arrangements that will improve forces available to support the plan. If in the U.S. and its territories, the Department of Justice, Federal Bureau of Investigation (FBI) is responsible for coordinating all Federal agencies and DoD forces assisting in the resolution of a terrorist incident. If outside the U.S. and its territories, the Department of State (DOS) is the lead agency. This information can be included in a separate Annex(s). See Annex A (Task Organization) and Annex J (Command Relationships).

d. Attachments/Detachments. ENTER installation/civilian agencies NOT normally assigned to the installation that are needed to support this plan. Explain interagency relationships and interoperability issues. This can be listed in other Annexes. See Annex A (Task Organization) and Annex J (Command Relationships).

e. Assumptions. (List planning/execution assumptions) ENTER all critical assumptions used as a basis for this plan. Assumptions are those factors unlikely to change during the implementation of the AT plan and that must be addressed in order to continue to plan. They can range from the installation's troop strength to addressing the local political/social environment. Examples follow:

(1) The installation is vulnerable to theft, pilferage, sabotage, and other threats. The installation is also vulnerable to a WMD attack.

(2) An act of terrorism involving WMD can produce major consequences that will overwhelm almost immediately the capabilities of the installation.

(3) Security personnel, both military and civilian, may be insufficient to provide total protection of all installation resources;

therefore, the principal owner or user of a facility, resource, or personnel must develop adequate unit awareness and safeguard measures.

(4) No single unit on the installation possesses the expertise to act unilaterally in response to WMD attacks.

(5) If protective equipment is not available, responders will not put their own lives at risk.

(6) Local, non-military response forces will arrive within [time] of notification.

(7) Units specializing in WMD response will arrive on-site within [number of hours based on installation location] of notification.

(8) The HN is supportive of U.S. policies, and will fulfill surge requirements needed to respond to a WMD incident IAW MOAs/MOUs.

f. Intelligence. ENTER the person, staff, or unit responsible for intelligence collection and dissemination. The installation commander must have a system in place to access current intelligence. This can be included in Annex B (Intelligence). National-level agencies, Combatant Commanders, and intelligence systems provide theater or country threat levels and threat assessments. In the U.S. and its territories, local installations must obtain the local terrorist threat information by querying the FBI through the installation's law enforcement liaison, local law enforcement, or other federal agencies. Obtain these assessments, as they will serve as a baseline for the installation's tailored assessment. The installation should have a process in place for developing the installation's tailored threat assessment or "local threat picture". The installation's tailored threat assessment should be continuously evaluated, updated, and disseminated, as appropriate, and as directed by the installation commander. The commander should determine the frequency and the means of dissemination of the installation's tailored AT product. Note: Commanders cannot change the threat level, which is developed at the national-level although they can declare higher FPCONs than the baseline.

2. MISSION. ENTER a clear, concise statement of the command's mission and the AT purpose or goal statement supporting the mission. The primary purpose of the AT plan is to safeguard personnel, property, and resources during normal operations. It is also designed to deter a terrorist threat, enhance security and AT awareness, and to assign AT responsibilities for installation personnel.

3. EXECUTION

a. Commander's Intent. Commander's vision on how he/she sees the execution of the unit's AT program. Refer to Service planning doctrine for assistance.

b. Concept of Operations. ENTER how the overall AT operation should progress. This plan stresses deterrence of terrorist incidents through preventive and response measures common to all combatant commands and Services. During day-to-day operations, the installation should stress continuous AT planning and passive, defensive operations. This paragraph should provide subordinates sufficient guidance to act if contact or communications with the installation chain of command is lost or disrupted.

(1) The installation's AT Concept of Operations should be phased in relation to pre-incident actions and post-incident actions. AT planning and execution requires that staff elements work with a much greater degree of cohesiveness and unity of mission than that required during the conduct of normal base sustainment operations. The AT mission, and the unpredictability of its execution, requires very specific "how to" implementation instructions of DoD FPCON Measures and in what manner these actions must be coordinated. This "how to" element is not normally included in the Concept of Operations paragraph; however the necessity to provide "how to" guidance in the AT plan requires a different manner of data presentation to ensure brevity and clarity. The implementation instructions are put into the form of action sets and can be displayed in the form of an execution matrix (Pre-Incident Action Set Matrix).

(2) In Post-Incident planning, the installation should focus on its response and reconstitution responsibilities upon notification of a terrorist incident and the procedures for obtaining technical assistance/augmentation if the incident exceeds the installation's organic capabilities. National-level responders (Federal Emergency Management Agency (FEMA), Red Cross, and Federal Bureau of Investigation (FBI)) may not be immediately accessible or available to respond to an installation's needs. Therefore each installation must plan for the worst-case scenario, by planning its response based on its organic resources and available local support through MOA/MOUs.

(3) The situation may dictate that the installation not only conduct the initial response but also sustained response operations. Many installations do not have onboard WMD officers or response elements. This paragraph will include specific implementation instructions for all functional areas of responsibility and the manner in which these actions must be coordinated. The implementation instructions can be put in the form of actions sets and displayed in the form of a synchronization matrix (Post-Incident Action Set Synchronization Matrix). The synchronization matrix format clearly describes relationships between activities, units, supporting functions, and key events which must be carefully synchronized to minimize loss of life and to contain the effects of a terrorist incident.

c. Tasks. ENTER the specific tasks for each subordinate unit or element listed in the Task Organization paragraph. Key members of the installation have responsibilities that are AT and/or WMD specific. The commander should ensure that a specific individual/unit/element within the installation is responsible for each action identified in this plan. Each individual/unit/element must know the tasks and responsibilities, what these responsibilities entail, and how these will be implemented. While the tasks and responsibilities for each AT planning and response Element will be delineated in the Pre- and Post-incident Action Set Matrices, it is recommended that the installation commander identify/designate the primary lead for each element and enter that information in this paragraph.

(1) First Subordinate Unit/Element/Tenant

(a) Task listing.

d. Coordinating Instructions. This paragraph should include AT specific coordinating instructions and subparagraphs, as the commander deems appropriate. In addition, this section of the AT plan outlines aspects of the installation's AT posture that require particular attention to guarantee the most effective and efficient implementation of the AT plan. For the

purposes of this plan, there are five basic coordinating instructions: 1) AT planning and response elements; 2) Procedural; 3) Security Posture; 4) Threat Specific Responsibilities; and 5) Special Installation Areas. The reader will be directed to specific Annexes that will provide amplifying instructions on these topics. The sections listed below are representative, and may not be all-inclusive.

(1) AT Planning and Response. For instructional purposes, this template outlines AT planning and response elements on the installation required to respond to a terrorist/WMD incident. Initial and sustained response to an attack must be a coordinated effort between the many AT planning and response elements of the installation, based on the installation's organic capabilities. As the situation exceeds the installation's capabilities, it must activate MOAs/MOUs with the local/State/Federal agencies (U.S. and its territories) or HN (outside the U.S. and its territories). For the purposes of this plan, an installation's capability is divided into AT planning and response elements. These tailored, installation-level elements parallel the national-level FEMA ESFs and the JSIVA evaluation criteria to the greatest degree possible.

AT PLANNING & RESPONSE ELEMENTS

Information & Planning	*	
Communications	*	+
HAZMAT	*	
Security	*	+
Explosive Ordnance Disposal (EOD)		+
Firefighting	*	+
Health & Medical Services	*	+
Resource Support	*	
Mass Care	*	
Public Works	*	
Intelligence Process		+
Installation AT Plans/Programs		+
Installation Perimeter Access		+
Security System technology		+
Executive Protection		+
Response & Recovery		+
Mail Handling		+

* Derived from FEMA ESFs

+ Derived from JSIVA assessment criteria

(2) Procedural

(a) Alert Notification Procedures. See Appendix 14 to Annex C (Operations).

(b) Use of Force/Rules of Engagement. See Annex H (Legal).

(c) Installation Training & Exercises. See Annex N (AT Program Review, Training & Exercises).

(d) Incident Response. See Appendix 1 to Annex C (Operations).

(e) Consequence Management. See Appendix 1 to Annex C (Operations).

(f) High-Risk Personnel Protection Procedures. See Appendix 9 to Annex C (Operations).

(g) AT Program Review (See Annex N (AT Program Review, Training & Exercises)).

(h) Higher Headquarters Vulnerability Assessments. See Annex N (AT Program Review, Training & Exercises).

(3) Security Posture Responsibilities

(a) Law Enforcement. See Appendix 7 to Annex C (Operations).

(b) Physical Security to include Lighting, Barriers, Access Control. See Appendix 6 to Annex C (Operations).

(c) Other On-site Security Elements. See Appendix 8 to Annex C (Operations).

(d) Operations Security. See Appendix 10 to Annex C (Operations).

(e) Technology. See Appendix 15 to Annex C (Operations).

(f) EOC Operations. See Appendix 12 to Annex C (Operations)

(g) Critical Systems Continuity of Operations (optional). See Appendix 13 to Annex C (Operations).

(h) Other

(4) Threat Specific Responsibilities

(a) Antiterrorism. See Appendix 2 to Annex C (Operations).

(b) Weapons of Mass Destruction. See Appendix 5 to Annex C (Operations).

(c) Special Threat Situations. See Appendix 3 to Annex C (Operations).

(d) Information Security. See Appendix 11 to Annex C (Operations).

(e) Natural/Man-made Hazards (Optional). See Appendix 16 to Annex C (Operations).

(f) Other.

(5) Special Security Areas

(a) Airfield Security. See Appendix 4 to Annex C (Operations).

(b) Port Security. See Appendix 4 to Annex C (Operations).

(c) Embarkation/Arrival Areas. See Appendix 4 to Annex C (Operations).

(d) Buildings. See Appendix 4 to Annex C (Operations).

(e) Other.

4. ADMINISTRATION AND LOGISTICS. ENTER the administrative and logistics requirements to support the AT plan, which should include enough information to make clear the basic concept for planned logistics support. Ensure the staff conducts logistical planning for both pre- and post-incident measures addressing the following: locations of consolidated WMD defense equipment; expedient decontamination supplies; Individual Protective Equipment exchange points; special contamination control requirements; retrograde contamination monitoring sites; WMD equipment/supply controlled supply rates and pre-stockage points; and procedures for chemical defense equipment "push" packages. Specific logistics and administrative requirements will emerge throughout the planning process outlined in the Concept of Operations, specifically when developing the action sets. These requirements should be incorporated into this paragraph. Finally, include fiscal instructions on how to support AT operations.

a. Administration. See Annex O (Personnel Services).

b. Logistics. See Annexes D (Logistics) and E (Fiscal).

5. COMMAND AND SIGNAL. ENTER instructions for command and operation of communications-electronics equipment. Identify the primary and alternate locations of the command post and emergency operations center. Enter the installation's chain of command. Highlight any deviation from that chain of command that must occur as a result of a WMD incident. The chain of command may change based on the deployment of a Joint Task Force or a National Command Authority-directed mission. Identify the location of any technical support elements that could be called upon in the event of a terrorist WMD incident and the means to contact each. Recommend the installation coordinate with higher headquarters to establish procedures to allow for parallel coordination to report a terrorist WMD incident. The installation must provide for prompt dissemination of notifications and alarm signals, and the timely/orderly transmission and receipt of messages between elements involved in and responding to the incident.

a. Command. See Annex A (Task Organization) and Annex J (Command Relationships).

b. Signal. See Annex K (Communications).

c. Command Post Locations

(1) Primary: ENTER location

(2) Alternate: ENTER Location

d. Succession of Command

(1) First alternate: ENTER position/title

(2) Second alternate: ENTER position/title

//SIGNATURE//

Commanding General/Officer
Signature Block

ANNEXES should provide amplifying instructions on specific aspects of the plan. Each ANNEX can be sub-divided into APPENDICES, TABS, and ENCLOSURES as required to provide amplifying instructions. Further, some of these supporting documents may be established in other unit operating orders/procedures, and referenced as required.

ANNEX A - Task Organization. ENTER key AT organization composition i.e., AT Working Group, Crisis Management Team, Emergency Operations Center, First Response Elements, etc.

Appendix 1 - Table of Organization

Appendix 2 - Post Prioritization Chart

ANNEX B - Intelligence. ENTER the agency(ies) responsible for intelligence and specific instructions. In the U.S. and its territories, commanders must obtain the local terrorist threat information by querying the FBI through the installation's law enforcement liaison, local law enforcement or other federal agencies

Appendix 1 - Local Threat Assessment

Appendix 2 - Local WMD Assessment

Appendix 3 - Local Criticality/Vulnerability Assessment

Appendix 4 - Risk Assessment

Appendix 5 - Pre-deployment AT Vulnerability Assessment

ANNEX C - Operations. This is the most IMPORTANT part of the plan. Annex C and supporting Appendices will provide specific instructions for all the various AT operations. All other Annexes/Appendices support the implementation of Annex C.

Appendix 1 - Incident Planning and Response. ENTER how the various agencies (military/civilian) and resources will be integrated to respond to the operations outlined below. These instructions should be generic enough to apply across the operational spectrum. Specific instructions for each operation will be detailed in the appropriate Annex/Appendix/Enclosure.

Tab A - Incident Command and Control Procedures

Tab B - Incident Response Procedures

Tab C - Consequence Management Procedures

Appendix 2 - Antiterrorism

Tab A - Mission Essential Vulnerable Assets (MEVA)

Tab B - Potential Terrorist Targets

Tab C - FPCON

Enclosure 1 - FPCON Action Sets (Who/What/When/Where/How)

Tab D - Random Antiterrorism Measures (RAM) Procedures

Appendix 3 - Special Threat Situations

Tab A - Bomb Threats

Enclosure 1 - Bomb Threat Mitigation

Enclosure 2 - Evacuation Procedures

Enclosure 3 - Search Procedures

Tab B - Hostage Barricaded Suspect

Tab C - Mail Handling Procedures

Appendix 4 - Special Security Areas

Tab A - Airfield Security

Tab B - Port Security

Tab C - Embarkation/Arrival Areas.

Tab D - Buildings

Appendix 5 - Weapons of Mass Destruction (CBRNE) & HAZMAT. ENTER the specific procedures planning, training, and response to WMD (CBRNE) incidents. Care should be taken to integrate existing plans for response to HAZMAT incidents to avoid duplication. Include "baseline" preparedness.

Tab A - WMD Action Set Synchronization Matrix (Who/What/Where/When/How)

Tab B - CBRNE Emergency Responder Procedures

Appendix 6 - Physical Security

Tab A - Installation Barrier Plan. ENTER procedures and pictorial representation of barrier plan.

Tab B - Installation Curtailment Plan

Tab C - Construction Considerations

Tab D - Facility and Site Evaluation and/or Selection

Tab E - AT Guidance for Off-Installation Housing

Appendix 7 - Law Enforcement

Tab A - Organization, training, equipping of augmentation security forces

Tab B - Alternate Dispatch Location

Tab C - Alternate Arming Point

Appendix 8 - Other On-Site Security Forces

Appendix 9 - High Risk Personnel

Tab A - List of High Risk Billets

Appendix 10 - Operations Security

Appendix 11 - Information Security

Appendix 12 - Emergency Operations Center (EOC) Operations. ENTER procedure for the activation & operations of the EOC.

Tab A - EOC Staffing (Partial/Full)

Tab B - EOC Layout

Tab C - EOC Messages & Message Flow

Tab D - EOC Briefing Procedures

Tab E - EOC Situation Boards

Tab F - EOC Security and Access Procedures

Appendix 13 - Critical Systems Continuity of Operations Plans (Optional). ENTER those systems that are essential to mission execution and infrastructure support of the installation i.e., utilities systems, computer networks, etc. This document outlines how the installation will continue to operate if one or more critical systems are disrupted or fails and how the systems will be restored.

Tab A - List of installation critical systems

Tab B - Execution checklist for each critical system

Appendix 14 - Emergency Mass Notification Procedures. ENTER the specific means and procedures for conducting a mass notification. Also covered should be the procedures/means for contacting key personnel and agencies.

Tab A - Situation Based Notification

Tab B - Matrix List of Phone Numbers/Email Accounts

Appendix 15 - Exploit Technology Advances. ENTER the process and procedures for developing and employing new technology. Identify who is responsible and what should be accomplished.

Appendix 16 - Higher Headquarters Vulnerability Assessments. ENTER procedures for conducting higher headquarters vulnerability assessments.

Appendix 17 - Natural/Man-made Hazards (Optional). Hurricanes, Flooding, Chemical Plants etc.

Tab A - Locality specific natural and man-made hazards

ANNEX D - Logistics (Specific logistics instructions on how to support AT operations)

Appendix 1 - Priority of Work. ENTER the priority of employing scarce logistical resource.

Appendix 2 - Emergency Supply Services

Appendix 3 - Weapons and Ammunition Supply Services

Appendix 4 - Emergency Equipment Services

Appendix 5 - Evacuation Shelters

Appendix 6 - Generator Refueling Matrix

ANNEX E - Fiscal (Specific fiscal instructions on how to support AT operations from pre-incident through post-incident)

Appendix 1 - AT Program of Memorandum Budget Submission Instruction

Appendix 2 - Combating Terrorism Readiness Submission Instructions

Appendix 3 - Fiscal Management during Exigent Operations

ANNEX F - Tenant Commanders (Specific instructions on how tenant commands/agencies support AT operations)

Appendix 1 - Areas of Responsibility (Pictorial)

ANNEX G - Air Operations (Specific air instructions on how to support AT operations)

Appendix 1 - List of Landing Zones (Used for emergency medical evacuations or equipment/personnel staging areas)

Appendix 2 - LZ Preparation Procedures

ANNEX H - Legal. ENTER the jurisdictional limits of the installation's commander and key staff. Although the Department of Justice, Federal Bureau of Investigation (FBI), has primary law enforcement responsibility for terrorist incidents in the United States, the installation commander is responsible for maintaining law and order on the installation. For OCONUS incidents, the installation commander must notify the HN and the geographic combatant commander; the geographic combatant commander will notify the Department of State (DOS). Once a task force or other than installation support arrives on the installation, the agencies fall under the direct supervision of the local Incident Commander. In all cases, command of military elements remains within military channels. The installation should establish HN agreements to address the use of installation security forces, other military forces, and host-nation resources that clearly delineate jurisdictional limits. The agreements will likely evolve into the installation having responsibility "inside the wire or installation perimeter" and the HN having responsibility "outside the wire or installation

perimeter". There may be exceptions due to the wide dispersal of work and housing areas, utilities, and other installation support mechanisms that may require the installation to be responsible for certain areas outside of the installation perimeter.

Appendix 1 - Jurisdictional Issues

Appendix 2 - Use of Force and/or Rules of Engagement Instructions

Appendix 3 - Pictorial Representation of Installation Jurisdiction

ANNEX I - Public Affairs (Specific PAO instructions on how to support AT operations)

Appendix 1 - Command Information Bureau Organization & Operation

Appendix 2 - Local/Regional Media Contact Information

ANNEX J - Command Relationships (Provides specific guidance on command relationships and military/civilian interoperability issues during incident command and control)

Appendix 1 - AT Organizational Charts. Crisis Management Team, AT Working Group, First Responder Elements, Incident Command Organization (include civilian and other external agencies)

ANNEX K - Communications (Specific communications instructions on how to support AT operations. Include systems/procedures for SECURE and NON-SECURE communications means)

Appendix 1 - Installation AT Communication Architecture

Appendix 2 - Incident Command Communication Architecture

Appendix 3 - EOC Communication Architecture

Appendix 4 - Security Force Communication Architecture

Appendix 5 - Fire Department Communication Architecture

Appendix 6 - Medical Communication Architecture

Appendix 7 - Other Agencies

ANNEX L - Health Services (Specific medical instructions on how to support AT operations)

Appendix 1 - Mass Casualty Plan

Appendix 2 - Procedures for Operating with Civilian Emergency Medical Service and Hospitals

ANNEX M - Safety (Specific safety instructions on how to support AT operations)

ANNEX N - AT Program Review, Training, & Exercises

Appendix 1 - AT Program Review

Tab A - Local Assessments

Tab B - Higher Headquarters Assessments

Appendix 2 - AT Required Training

Appendix 3 - Exercises

ANNEX O - Personnel Services. ENTER administrative and personnel procedures required to support the plan i.e., civilian overtime, post-traumatic stress syndrome counseling.

Appendix 1 - Operating Emergency Evacuation Shelters

ANNEX P - Reports. ENTER all the procedures for report submissions & report format.

Appendix 1 - Reporting Matrix

ANNEX Q - References. ENTER all supporting reference materials, publication, regulations etc.

ANNEX R - Distribution. ENTER the list of agencies to receive this plan. Cover plan classification, handling and declassification procedures.

(This page intentionally left blank)

AT/CIP T&R MANUAL

APPENDIX H

TERRORIST INCIDENT RESPONSE MEASURES CHECKLIST

(This appendix is not intended to be doctrinal in nature but rather a tool for Commanders and ATOs to use when building, evaluating, and improving their antiterrorism programs.)

INTRODUCTION. The antiterrorism success of each unit operating within a Combatant Command shall depend on the degree and seriousness of the crisis management planning. The following checklist identifies items that should be considered for inclusion into the crisis management plan prepared for each unit, activity, installation, or organization as appropriate.

Table 5.T1. Terrorist Incident Response Checklist

Intelligence	
	Does the plan allow for the intelligence-gathering process (e.g., collection, evaluation, and dissemination of information) to aid in the identification of the local threat?
	Does the plan consider restrictions placed on the collection and storage of information?
	Does the plan indicate an awareness of sources of information for the intelligence-gathering effort (e.g., military intelligence, federal agencies, state/local authorities)?
	Does the plan allow for liaison and coordination of information (e.g., establishing a threat committee)?
Threat Analysis	
	Does the plan identify the local threat (immediate and long-term)?
	Does the plan identify other threats (e.g., national and international groups who have targeted or might target US installations)?
	Does the installation incorporate factors of the installation vulnerability determining system when assessing the threat?
	Does it address:
	Geography of the area concerned.
	Law enforcement resources.
	Population factors.
	Communications capabilities.
	Does the plan establish a priority of identified weaknesses and vulnerabilities?
Security Countermeasures	
	Does the plan have specified FPCONs and recommended actions/measures?
	Do security countermeasures include a combination of physical operations and sound-blanketing security measures?
Operations Security	
	Have procedures been established that prevent terrorists from readily obtaining information about plans and operations (e.g., not publishing the commanding general's itinerary, safeguarding classified material, etc.)?
	Does the plan allow for in-depth coordination with the installation's OPSEC program?
	Has an OPSEC annex been included in the contingency plan?

Personnel Security	
	Has an education process been started that identifies threats to vulnerable personnel?
	Has the threat analysis identified individuals vulnerable to terrorist attack?
	Has a school trained AT Officer been designated in writing.
Physical Security	
	Are special threat plans and physical security plans mutually supportive?
	Do security measures establish obstacles to terrorist activity (e.g., guards, host nation forces, lighting, fencing)?
	Does the special threat plan include the threats identified in the threat statements of higher headquarters?
	Does the physical security officer assist in the threat analysis and corrective action?
	Is there obvious command interest in physical security?
	Does the installation have and maintain detection systems and an appropriate assessment capability?
Security Structure	
	Does the plan indicate that the FBI has primary domestic investigative and operational responsibility?
	Has coordination with the staff judge advocate been established?
	Does the plan allow for close cooperation between principal agents of the military, civilian, and host nation communities and federal agencies?
	Does the plan clearly indicate parameters for use of force, including the briefing of any elements augmenting military police assets?
	Is there a mutual understanding between all local agencies (e.g., military, local FBI resident or senior agent-in-charge, host nation forces and local law enforcement) that might be involved in a terrorist incident on the installation regarding authority, jurisdiction, and possible interaction?
	Has the staff judge advocate considered ramifications of closing the post (e.g., possible civilian union problems)?
Emergency Operations Center (EOC) Training	
	Has the EOC been established and exercised?
	Is the EOC based on the needs of the installation while recognizing manpower limitations, resource availability, equipment, and command?
	Does the plan include a location for the EOC?
	Does the plan designate alternate locations for the EOC?
Emergency Operations Center (EOC) Training (cont.)	
	Does the plan allow for the use of visual aids (e.g., chalkboards, maps with overlays, etc.) to provide situation status reports and countermeasures?
	Does the plan create and designate a location for a media center?
	Have the EOC and media center been activated together within the last quarter? If not provide date of the last activation.
	Does the EOC have SOPs covering communications and reports to higher headquarters?
Reaction Force Training	
	Has the reaction force been formed, equipped (including CBRNE

	equipment) and mission-specific trained (e.g., building entry and search techniques, vehicle assault operations, anti-sniper techniques, equipment)?
	Has the force been briefed on laws and policies governing the use of force and the use of deadly force in the protection of DoD personnel, facilities, and materiel?
	Has the force been trained and exercised under realistic conditions?
	Has corrective action been applied to shortcomings/deficiencies?
	Has the reaction force been tested quarterly (alert procedures, response time, overall preparedness)?
	Has responsibility been fixed for the negotiation team? Has the negotiation team been trained and exercised under realistic conditions?
General Observations	
	Was the plan developed as a coordinated staff effort?
	Does the plan outline reporting requirements (e.g., logs, journals, after-action report)?
	Does the plan address controlled presence of the media?
	Does the plan include communications procedures and communications nets?
	Does the plan consider the possible need for interpreters?
	Does the plan consider the need for a list of personnel with various foreign backgrounds to provide cultural intelligence on foreign subjects and victims, as well as to assist with any negotiation efforts?
	Does the plan provide for and identify units that shall augment military police assets?
	Does the plan delineate specific tasking(s) for each member of the operations center?
	Does the plan provide for a response for each phase of antiterrorism activity (e.g., initial response, negotiation, assault)?
	Does the plan designate service support requirements (e.g., engineer, aviation, medical, communications, etc.)?
	Does the plan make provisions for notification of nuclear assessment teams and the nuclear accident/incident control officer?
	Does the plan provide for explosive ordnance disposal (EOD) support?
General Observations (cont.)	
	Does the plan take into consideration the movement from various locations, including commercial airports, of civilian and military advisory personnel with military transportation assets?
	Does the plan allow for the purchase and/or use of civilian vehicles, supplies, food, etc., if needed (including use to satisfy a hostage demand)? Does the plan make provisions for paying civilian employees overtime if they are involved in a special threat situation?
	Does the plan take into consideration the messing, billeting, and transportation of civilian personnel?

(This page intentionally left blank)

AT/CIP T&R MANUAL

APPENDIX I

TERRORIST SURVEILLANCE DETECTION

(This appendix is not intended to be doctrinal in nature but rather a tool for Commanders and ATOs to use when building, evaluating, and improving their antiterrorism programs.)

INTRODUCTION. This enclosure provides guidance for Commanders and ATOs to stress the importance of overt terrorist surveillance detection efforts by military police forces to deter terrorist surveillance activities.

a. The recent increase in reporting of suspicious individuals conducting surveillance of U.S. military and civilian sites in the United States and overseas indicates possible pre-operational targeting by terrorists and merits attention by Commanders at all levels. The persistent stream of reports necessitates Commanders and security planners to understand the purpose of terrorist surveillance, know what terrorists look for, and know how they conduct surveillance operations. With this basic knowledge, Commanders can then implement protective countermeasures, comply with DoD standardized reporting procedures, and in the end deter, detect, disrupt, and defend against future terrorist attacks.

TERRORIST SURVEILLANCE

a. Vulnerability Assessment. Terrorists conduct surveillance to determine a target's suitability for attack by assessing the capabilities of existing security systems and discerning weaknesses for potential exploitation. Terrorists closely examine security procedures, such as shift changes, access control, and roving patrols; citizenship of security guards; models and types of locks; presence of closed-circuit cameras; and guard dogs. After identifying weaknesses, terrorists plan their attack options at the point or points of greatest vulnerability.

b. Terrorist Surveillance Techniques. The basic methods of surveillance are "mobile" and "fixed" (or static).

(1) Mobile surveillance entails active participation by the terrorists or operatives conducting surveillance, usually following as the target moves. Terrorists conduct mobile surveillance on foot, in a vehicle, or by combining the two. Mobile surveillance usually progresses in phases from a stakeout, to a pick up and then through a follow phase until the target stops. At this point operatives are positioned to cover logical routes to enable the surveillance to continue when the target moves again.

(2) Terrorists conduct fixed or static surveillance from one location to observe a target, whether a person, building, facility, or installation. Fixed surveillance often requires the use of an observation point to maintain constant, discreet observation of a specific location. Terrorists establish observation posts in houses, apartments, offices, stores, or on the street. A mobile surveillance unit, such as a parked car or van, can also serve as an observation post. Terrorists often park outside a building, facility, or installation to observe routines of security and personnel coming and going. Terrorists also use various modes of transportation to include buses, trains or boats or move by foot to approach and observe installations.

(3) Protective Countermeasures.

(a) The incorporation of visible security cameras, motion sensors, working dog teams, random roving security patrols (varying size, timing, and routes), irregular guard changes, and active searches (including x-ray machines and explosive detection devices) of vehicles and persons at entry points shall improve a facilities' situational awareness and present a robust force protection posture that dramatically inhibits terrorist surveillance efforts.

(b) The emplacement of barriers, roadblocks, and entry mazes that are covered by alert security forces shall provide additional deterrence as these measures increase standoff and improve security force reaction time in the event of an attack.

(c) The implementation of unannounced random security measures such as 100 percent identification of all personnel entering the facility or installation, conducting inspections and searches of personnel and vehicles, and visible displays of vehicles mounted with crew served weapons shall increase uncertainty and thus the risk of failure in the minds of terrorists.

(d) Surveillance Detection. Because terrorists must conduct surveillance - often over a period of weeks, months, or years - detection of their activities is possible. Regardless of the level of expertise, terrorists invariably commit mistakes. Knowing what to look for and being able to distinguish the ordinary from the extraordinary are keys to successful surveillance detection. For these reasons, overt surveillance detection in its most basic form is simply watching for persons observing personnel, facilities, and installations.

1. The objectives of overt surveillance detection measures are to record the activities of persons behaving in a suspicious manner and to provide this information in a format useable by the appropriate law enforcement or intelligence officials. It is important to note that overt surveillance detection emphasizes the avoidance of interpersonal confrontations with suspicious individuals unless exigent situations necessitate otherwise. Depending upon the circumstances or trends, Commanders and senior law enforcement officials in coordination with intelligence experts through installation threat working groups may determine the need for more specialized covert counter surveillance measures to assure installation protection.

2. For surveillance detection efforts to achieve positive results, military police/security forces should immediately report incidents of surveillance and suspicious activities by providing detailed descriptions of the people, the times of day, the locations, the vehicles involved, and the circumstances of the sightings to their respective criminal investigative services or counterintelligence elements for incorporation into reports such as U.S.A.F. TALON or the NCIS Suspicious Incident Report. The incident reports are important pieces of information that over time combined with other similar sightings allow investigators to assess the level of threat against a specific facility, installation, or geographic region.

3. The emphasis of surveillance detection is on indicators and warnings of terrorist surveillance activities. Surveillance detection

efforts should focus on recording, then reporting incidents similar to the following:

- a. Multiple sightings of the same suspicious person, vehicle, or activity, separated by time, distance, or direction.
- b. Possible locations for observation post use.
- c. Individuals who stay at bus and/or train stops for extended periods while buses/trains come and go.
- d. Individuals who carry on long conversations on pay or cellular telephones.
- e. Individuals who order food at a restaurant and leave before the food arrives or who order without eating.
- f. Joggers who stand and stretch for an inordinate amount of time.
- g. Individuals sitting in a parked car for an extended period of time.
- h. Individuals who don't fit into the surrounding environment by wearing improper attire for the location (or season).
- i. Individuals drawing pictures and/or taking notes in an area not normally of interest to a standard tourist or showing interest in or photographing security cameras, guard locations, or noticeably watching security reaction drills and procedures.
- j. Individuals who exhibit unusual behavior such as staring or quickly looking away from individuals or vehicles as they enter or leave designated facilities or parking areas.
- k. Terrorists may also employ aggressive surveillance by false phone threats, approaching security checkpoints to ask for directions or "innocently" attempting to smuggle non-lethal contraband through checkpoints. Clearly the terrorists intend to determine firsthand the effectiveness of search procedures and to gauge the alertness and reaction of security personnel.

4. It is important to highlight that the above surveillance indicators are recorded overtly and while performing normal military police/security forces activities. The intent is to raise the awareness of our military police/security forces to record and report the unusual during the course of routine law enforcement and security duties.

5. Reporting Terrorist Surveillance Indicators. Implementing effective security countermeasures and employing overt surveillance detection principles shall deter terrorist surveillance. However, regardless of the capabilities of a facility or installation to resource antiterrorism protective measures, good working relationships with local, State, and Federal law enforcement agencies are essential to establishing cohesive, timely and effective responses to the indicators of terrorist activity.

a. Installation Commanders and senior law enforcement officials should coordinate and establish partnerships with local authorities (i.e. installation threat working groups) to develop intelligence and information sharing relationships to improve security for the installation and the military community at large.

b. For those occasions when the indicators of terrorist surveillance continue despite well executed overt security countermeasures the objectives should be to provide detailed reports of the indicators of surveillance to the appropriate law enforcement agency or intelligence activity. As reports of suspicious activity increase and the trends clearly indicate pre-operational terrorist surveillance, it may be necessary for installation Commanders in coordination with senior law enforcement and intelligence officials to implement more sophisticated, uniquely tailored counter surveillance solutions and assets to investigate the circumstances.

c. Specialized counter surveillance assets should be coordinated and vetted by forwarding requests through the chain of command via pre-determined service or combatant command request procedures.

AT/CIP T&R MANUAL

APPENDIX J

AT SECURITY CONSIDERATIONS FOR THE CONTRACTING PROCESS

(This appendix is not intended to be doctrinal in nature but rather a tool for Commanders and ATOs to use when building, evaluating, and improving their antiterrorism programs.)

INTRODUCTION

a. Contracting for support services is a normal, ever expanding function of providing essential logistical services within the Department of Defense. Contracting for services present AT security challenges (which, if not addressed) could create seams and gaps in a unit's overall security profile. The Federal Acquisition Regulations (FAR) is the principle guidance used to establish Federal Government contracts and provides explicit directions for contract requirements, award, execution, and evaluation. At OCONUS locations, SOFA, MOA, and other documents shall prescribe guidance for the contracting process with regard to host nation service providers. ATOs should work closely with the contracting officer and the legal officer to ensure AT security considerations are properly and legally incorporated into the contracting process. Each Combatant Commander should consider developing AOR and/or country specific, AT security guidance for the contract process based on their individual threat concerns and agreements with host nations.

b. References do not specifically prohibit or prescribe AT security considerations for contracts. It is the responsibility of the commander to incorporate AT security considerations into the contracting process. This appendix shall offer an AT process that can be used to incorporate AT security considerations into the contracting process. It also suggests specific AT security measures that can be employed.

INCORPORATING AT SECURITY CONSIDERATIONS INTO THE CONTRACTING PROCESS

a. Commanders are responsible for ensuring AT security measures are included into the contracting process. Each commander should develop area specific, AT security guidance and incorporate the same into their AT program. This Commander's guidance forms are the core AT security criteria that shall be applied to all contracts as a baseline. Contract AT security considerations should be considered during the commander's AT risk assessment process. This process results in the acceptance of a level of AT risk and parameters; or in the investment of additional AT security costs.

b. The ATO and the contracting officer are responsible for ensuring the application of the Commander's guidance. This ensures AT security measures are included into the statement of work (SOW) and if applicable, the [DD Form 254](#), Contracting Certification Specification. It is the contracting officer's responsibility to ensure the contract is prepared IAW appropriate contracting regulations and guidance. It is important to include the AT working group and host nation representatives as required throughout this process. Listed below is a step-by-step process for considering AT security into contracts. Table 8.T1 also outlines the process for incorporating AT security considerations into the logistics contract process.

c. Determine the Contract Requirement. The unit requiring the contract service is responsible for identifying the specific contract requirement. The unit shall work with the contracting officer to ensure the framework of the contract/scope of work is properly constructed. This is done within the Department of Defense, Service, Combatant Commander, FAR, and contracting guidance. It is at this step that the unit should determine how essential this contract service is to mission accomplishment. Are there alternative means to providing the contract service without mission degradation? It is important to determine the scope of the contract, who shall execute the contract, what unit (s) shall be affected by it, when it shall be executed (timeframe), where it shall be executed, and what the area/building access requirements are. The concern during this step is to determine the specific logistics requirement (s), not determining AT security considerations.

d. Conduct AT RA. The unit shall conduct an AT risk management process using locally prepared AT assessments (Threat, Criticality, Vulnerability, and Risk). The use of these products shall help the unit in assessing and identifying the potential AT risks associated with the contract and the incorporation of specific AT security countermeasures. Part of this process is to consider alternative means of fulfilling the contract requirement as a means to mitigate or eliminate risks. The ATO shall assist in the AT risk management process; ensuring local security measures are leveraged and/or modified against risks/vulnerabilities associated with the contract.

e. Determine AT Security Requirements. During this step, the ATO shall assist the unit in the development of specific AT security measures. AT security measures should be based on an AT RA and reflect the Commander's overall AT risk management strategy. There should be a balance between effective security measures and cost-benefit. The unit and the ATO should apply the Commander's AT security considerations during this step. The ATO should craft AT security strategies that complement the existing security profile of the location from a normal security posture through advanced readiness postures. Flexibility should be incorporated into the contract to allow for random schedules, access and/or search requirements, and changes in the local threat. For example, contractor personnel may be directed to enter the location through certain access points where they can best be identified and searched. Contractor personnel may be prohibited from certain portions of the location and during advanced readiness postures. Contract services may be curtailed or more closely supervised.

Table 8.T1 Process for Considering AT Security Measures into Contracts

Step	Major Tasks	OPR
Determine Contract Requirements	<ul style="list-style-type: none"> - Determine contract support requirement. - Comply with applicable DoD and Service FAR guidance and Combatant Commander contracting guidance. - Determine scope of contract. 	Unit and Contracting Officers
Perform AT Risk Analysis	<ul style="list-style-type: none"> - Conduct AT risk analysis. - Leverage local risk analysis information. - Determine risks associated with contract. - Develop logistics alternatives...balanced with mission accomplishment. 	Unit and AT Officer
Determine AT Security Measures	<ul style="list-style-type: none"> - Develop specific AT security measures. - Leverage and/or modify security measures. - Develop range of security measures...normal through advanced readiness postures. 	AT Officer and Unit

Step	Major Tasks	OPR
	<ul style="list-style-type: none"> - Include AT security requirements in SOW and DD Form 254. - Consider linkage with local FPCON system. - Balance between security and cost-benefit. 	
Build Contract	<ul style="list-style-type: none"> - Incorporate contract requirement(s) and security measures into written contract. - Staff contract. - Commander endorsement of security measures and acceptance of risk. 	Unit and Contracting Officer
Award/Execute Contract	<ul style="list-style-type: none"> - Select and screen contractors. - Incorporate contract security requirements into unit AT/FP plan. - Notify ATO contract is activated. - Ensure all AT security measures are in place before execution. 	Unit and Contracting Officer/AT Officer
Contract Review	<ul style="list-style-type: none"> - Periodically inspect AT security measures. - Review AT security measures should local threat change. - Annual, formal review upon contract renewal. 	Unit and Contracting Officer

Table 8.T2 below identifies some of the specific AT security measures that should be considered for the logistics contract process.

(1) Build Contract. This step involves combining the logistics requirement (s) with the AT security measure (s) into a written contract. As a minimum, the contract should be staffed through the AT Working Group, the legal officer, and the Commander. This is the Commander's formal endorsement that the AT security measures are satisfactory and he or she has accepted the AT risk.

(2) Award/Execute Contract. The unit should consider including contract security requirements as part of their unit's AT Plan to ensure proper coordination and synchronization with other AT activities. Once the contract is awarded, those security requirements become binding and should be in place. Any contractor personnel screening requirements should be met prior to starting the contract. The contracting officer and the unit should notify the ATO prior to the contract services starting so he can ensure all required AT security measures are in place.

(3) Contract Review. The unit should establish procedures to periodically review the effectiveness of the contract, both in terms of services rendered and AT security measures in place. Contract reviews should all be the day-to-day inspection/evaluation of services rendered, periodic inspection of access controls to ensure control procedures are not being abused, and a formal annual review process to renew or cancel the contract. A contract review should also be done if the local threat changes and/or there is a requirement to modify and renegotiate the terms of the contract.

Table 8.T2 AT Security Measures for Logistics Contracts

AT Security Area	AT Security Measure
Contractor Screening	- Pre-approved, reputable companies vetted through contracting office, Chief of Mission, DoD.

AT Security Area	AT Security Measure
	<ul style="list-style-type: none"> - Consider limiting the announcement for contractors to trusted sources based on sensitivity of the mission. - Background Check (Law Enforcement, Host Nation). - Screen company and prospective workers.
Access Control	<ul style="list-style-type: none"> - Defined process for replacement of workers. - Establish a central contractor database that is accessible to security forces and contains contractor ID with picture. - Limit work area. Clearly identify restricted/exclusion areas where contractor personnel are not authorized without specific permission or an escort. - Access control roster (personnel and vehicles). Names/vehicles verified by the company and received background screening, and/or host nation certification. Substitutes receive same vetting process prior to work. - Badge systems. - Exchange badge system. - Personal identification systems i.e., work uniform, vehicle marking. - Biometrics systems i.e., fingerprint, retinal, facial feature reading device. - Have large vehicles arrive empty before entering location i.e., trash trucks. - Arranging vehicle loads to facilitate searching. - Verify contents of large vehicles at distribution point and/or using an electronic vehicle-screening device. - Consider an alternate access control point for screening/search contractor personnel and vehicle. Especially oversize vehicles. - Consider an unloading zone away from protected assets. - Ensure host nation language translation support. - Coordinate host nation security requirements.
Circulation Control	<ul style="list-style-type: none"> - Designate authorized work areas and travel routes. - Provide easily identifiable coding for badges and vehicle. - Assign a unit escort (armed as required) to the contractor. - Deny access during increased readiness conditions.
Special Security Concerns	<ul style="list-style-type: none"> - Include contract services as part of the local risk analysis/management process. - Ensure AT security measures already in place are leveraged/complemented. - Consider all possible alternatives to fulfilling the required service. Is the service really required to accomplish the mission? - Consider time and space factors to allow determination of hostile intent into AT security measures. - Consider incorporating contractor security measures into the local FPCON system.

AT Security Area	AT Security Measure
	<ul style="list-style-type: none"> - Monitor contractor (s) at the work-site as required by security environment. - Review contracts annually or when the local threat changes. - Establish food and/or water testing protocols. - Identify and monitor food, water, and petroleum distribution points (on and off location). - Ensure delivery schedules are random and unpredictable. - Consider periodic interviews of contractors by security force personnel. - Provide contractor training and procedures for reporting suspicious activity and/or stolen equipment. - Determine what risks still remain after all AT security measures are applied...acceptance of risk. - Conduct frequent, random patrols, inspections, and spot-checks. - Establish a security response force. - Ensure host nation agreements allow for adequate AT security considerations during the logistics contracting process.

(This page intentionally left blank)

AT/CIP T&R MANUAL

APPENDIX K

FAMILY SECURITY QUESTIONS

(This appendix is not intended to be doctrinal in nature but rather a tool for Commanders and ATOs to use when building, evaluating, and improving their antiterrorism programs.)

INTRODUCTION

a. The following are questions that can be asked to help identify practices that may increase the likelihood that a DoD person or dependent shall become a victim of a kidnapping or other terrorist act.

HEAD OF HOUSEHOLD

a. Is your telephone number and address in local directories?

b. Do you, your family members, or your domestic employees answer your telephone with your name and rank?

c. Have you had a security check run on all domestic employees? If overseas, did you check with the MILGROUP and/or Embassy Regional Security Officer (RSO) to see if they have any program to help screen prospective employees' records? If not, contact the local military police/counterintelligence office or local police to obtain pre-employment screening assistance.

d. Have you maintained a file on each household employee including the full name, address, description, date and place of birth, current photograph and a full set of fingerprints (if allowed, host nation laws may prohibit the collection of some data on local nationals, i.e. fingerprints)?

e. Have outside fuse boxes/circuit breakers been modified so they can be locked at all times unless access is specifically required?

FAMILY

a. Have you adopted a family security program including duress codes and alarms, crime watch practices, and conscious efforts to avoid patterns in daily activities?

b. Have all family members learned emergency telephone numbers? Have they been able to memorize them? Do all family members know how to summon police in the local language? Are they aware or do they carry instructions in wallet cards on how to work local telephones and ask for assistance?

c. Have emergency numbers been posted near each telephone? Do these listings give away the nature of the family's assignment (Ambassador's home phone should not be listed, etc.). Have all family members been given a sanitized list of phone numbers they can carry with them at all times?

d. Do you have a system for keeping family members informed about each other's whereabouts at all times? Have you included a family duress or trouble signal as part of your family check-in system?

e. Have you removed all symbols or signs from the outside of your residence indicating nationality, rank or grade, title, and name?

f. Have you unnecessarily disseminated personal, family, and travel plans to casual acquaintances or domestic employees who do not need to know your personal schedule on an hourly or daily basis?

g. Have you learned and practiced emergency phrases in the local language such as "I need a policeman, a doctor, help, etc."? Have you written these down in transliteration as well as in the native language so you could show a 3 x 5 card to obtain assistance?

h. Do you and your family members know how to work local pay telephones? Does each family member carry a small quantity of money or phone cards necessary and sufficient to operate local pay telephones at all times? Alternatively, do family members carry cell phones?

i. Are residence doors and windows locked? Have additional security devices been added to door and window locks to increase resistance to intrusion and penetration?

j. Do you and your family members close draperies during periods of darkness? Are the draperies made of opaque, heavy material that provides maximum privacy (and can reduce the distribution of glass shards in the event windows are broken).

k. Have you considered obtaining a dog for protection of your house and grounds?

l. Do you avoid leaving a spare key in the mailbox or in a similar insecure place?

m. Are tools used by the family, particularly ladders, under lock?

n. Do you have a private place to leave notes for family members or do you tack notes on the door for family, friends, criminals, and terrorists to read?

o. Have you developed a response plan for yourself and family members in the event that an unauthorized person is suspected to be inside your home upon your return? Does your plan emphasize the need to contact the police or the security office immediately and discourage personal investigation of the possible intrusion?

p. Do you or family members automatically open the residence door to strangers? Do you or your family members use a peephole or CCTC monitor to identify callers? Do you request to see and verify credentials from utility, service, or other persons seeking to enter your residence?

q. Do you or your family members admit polltakers and salespersons to your home? Are you aware of the presence of peddlers and all strangers in your neighborhood? Are your family members equally aware? (Terrorists are known to have gathered substantial information relative to their victims using these deceptions.)

r. Have you and your family members reported frequent wrong numbers or nuisance telephone calls to the telephone company and the police? Have you considered that someone may be attempting to determine the presence of family members?

s. Have you reported the presence of strangers in the neighborhood? Does it appear that someone or some group may be trying to gain an intimate knowledge of your family's habits?

t. Do you and your family members watch for strange cars cruising or parked frequently in the area, particularly if one or more occupants remain in the car for extended periods? Have you made a note of occupants, license numbers and province designators of suspicious vehicles?

u. Do you discuss family activities with strangers?

v. Do you discuss family plans over the telephone?

w. Do you discuss detailed family or office plans over the telephone with people you do not personally know or know well?

x. Do you mail letters concerning family travel plans from your house or office? Are you sure that no one is intercepting your outbound mail, opening it, and then resealing it for delivery after collecting desired information enclosed in it?

y. Have you or family members accepted delivery of unordered or suspicious packages or letters?

z. Do you destroy all envelopes papers and other items that reflect your name, rank, SSN and other sensitive information?

aa. Have you limited publicity concerning yourself and your family, which may appear in local news media?

bb. Do you and your family shop on a set schedule? Do you and your family members always shop at the same stores? Do you and your family members always use the same routes to the office, to shopping, to school, and to after school activities?

cc. Do you have a coordinated family emergency plan? Have you ensured that all family members know who to contact if they suspect another family member is in danger? Have you reviewed protective measures with all family members?

dd. Have you made sure that each family member is prepared to evacuate the area quickly in the event of an emergency? Do you know where all critical documents such as passports, visas, shot and other medical records are kept? Are these current, and can you or other family members extract them from their secure storage place on very short notice?

ee. Do you find yourself in disputes with citizens of the host country over traffic, commercial transactions, or other subjects? Have you or your family members precipitated any incidents involving host country nationals?

CHILDREN

a. Have the children been instructed not only to refuse rides from strangers, but also to stay out of reach if a stranger in a car approaches them?

b. Have you located the children's rooms in a part of the residence that is not easily accessible from the outside?

c. Do you ever leave your children at home alone or unattended?

d. Are you sure that the person with whom you leave your children is responsible and trustworthy?

e. Are you sure that outside doors and windows leading into the children's rooms are kept locked, especially in the evening?

f. Have you taught your children the following?

(1) Never let strangers into your house.

(2) Avoid strangers and never accept rides from anyone that he/she does not know.

(3) Refuse gifts from strangers.

(4) Never leave home without telling an adult where and with whom you are going.

(5) How to call the police.

(6) To call the police if ever you are away and they see a stranger around the house.

(7) Whenever possible, walk on main thoroughfares.

(8) Tell you if he or she notices a stranger hanging around your neighborhood.

(9) Play in established community playgrounds rather than in isolated areas.

(10) Give a false name if ever asked by a stranger.

SCHOOLS

a. Have you asked schools attended by your children to:

b. Not give out any information on your students to anyone unless you specifically authorize them to do so in advance? To avoid any kind of publicity in which students are named or their pictures are shown.

c. Not to release a student to someone other than his/her parents without first receiving authorization from a parent.

d. To allow children to talk to a parent on the telephone in the presence of school officials before allowing an authorized release to

actually occur. (This practice provides protection against a kidnapper who calls and claims to be the child's parent.)

e. To report to the police if any strangers are seen loitering around the school or talking to students. If such strangers are in a car, the teacher should note its make, color, model, and tag number and pass this information on to the police.

f. To have teachers closely supervise outside play periods.

NEIGHBORS

a. Have you met your neighbors?

b. Have you gotten them interested in maintaining and improving neighborhood security?

c. Have you exchanged telephone numbers?

d. Have you established some sort of system for alerting one another to trouble in neighborhood?

STRANGERS

a. Have all family members and domestic employees been instructed on the requirement that maintenance work is to be performed only when scheduled by a parent unless a clear emergency exists?

b. Do you have procedures established on how to be contacted in the event that a utility emergency occurs and maintenance personnel must enter your residence?

c. Do your family members and domestic employees know how to verify the identity of maintenance personnel?

d. Have you and your family discussed the kind of assistance you can offer to a person who comes to your door claiming to be the victim of an automobile accident, a mechanical breakdown, or some other kind of accident?

e. Have you explained to your family they can offer to call the police, the fire department, or an ambulance, but under no circumstances should they allow the victim into the residence?

(This page intentionally left blank)

AT/CIP T&R MANUAL

APPENDIX L

HOUSEHOLD SECURITY CHECKLIST

(This appendix is not intended to be doctrinal in nature but rather a tool for Commanders and ATOs to use when building, evaluating, and improving their antiterrorism programs.)

INTRODUCTION. This generic household checklist should be used to evaluate current and prospective residences when a locally specific checklist is not available. Prospective renters should attempt to negotiate security upgrades as part of the lease contract when and where appropriate. This could reduce costs to the DoD member by amortizing costs over period of the lease.

EXTERIOR HOUSEHOLD SECURITY LIST

Yes/No

- _____ If you have a fence or tight hedge, have you evaluated it as a defense against intrusion?
- _____ Is your fence or wall in good repair?
- _____ Are the gates solid and in good repair?
- _____ Are the gates properly locked during the day and at night?
- _____ Do you check regularly to see that your gates are locked?
- _____ Have you eliminated trees, poles, ladders, boxes, etc., that might help an intruder to scale the fence, wall, or hedge?
- _____ Have you removed shrubbery near your gate, garage, or front door, which could conceal an intruder?
- _____ Do you have lights to illuminate all sides of your residence, garage area, patio, etc.?
- _____ Do you leave your lights on during hours of darkness?
- _____ Do you check regularly to see that the lights are working?
- _____ If you have a guard, does his post properly position him to have the best possible view of your grounds and residence?
- _____ Does your guard patrol your grounds during the hours of darkness?
- _____ Has your guard been given verbal or written instructions, does he understand them?
- _____ Do you have dogs or other pets that will sound an alarm if they spot an intruder?
- _____ Have you considered installation of a camera system with record capabilities or dummy camera system as a deterrent?

INTERIOR HOUSEHOLD SECURITY LIST

Yes/No

- _____ Are your perimeter doors made of metal or solid wood?
- _____ Are the doorframes of good solid construction?
- _____ Do you have an interview grill or optical viewer in your main entrance door?
- _____ Do you use the interview grill or optical viewer?
- _____ Are your perimeter doors properly secured with good heavy duty dead bolt locks?
- _____ Are the locks in good working order?
- _____ Can any of your door locks be by bypassed by breaking the glass or a panel of light wood?
- _____ Have you permanently secured all unused doors?
- _____ Are your windows protected by solid steel bars, ornamental or some other type of shutters?
- _____ Do you close all shutters at night and when leaving your residence for extended periods of time?
- _____ Are unused windows permanently closed and secured?
- _____ Are your windows locked when they are shut?
- _____ Are you as careful of second floor, or basement windows as you are of those on the ground floor?
- _____ Have you secured sliding glass doors with a broom handle "charlie bar," or good patio door lock?
- _____ If your residence has a skylight, roof latch, or roof doors, are they properly secured?
- _____ Does your residence have an alarm system?
- _____ Have you briefed your family and servants on good security procedures?
- _____ Do you know the phone number of the police security force that services your neighborhood?

GENERAL HOUSEHOLD SECURITY LIST

Yes/No

- _____ Are you and your family alert in your observations of persons who may have you under surveillance, or who may be casing your house in preparation for a burglary or other crime?
- _____ Have you verified the references of your servants, and have you submitted their names for security checks?
- _____ Have you told your family and servants what to do if they discover an intruder breaking into, or already in the house?
- _____ Have you restricted the number of house keys?
- _____ Do you know where all your house keys are?

(This page intentionally left blank)

AT/CIP T&R MANUAL

APPENDIX M

GROUND TRANSPORTATION SECURITY TIPS

(This appendix is not intended to be doctrinal in nature but rather a tool for Commanders and ATOs to use when building, evaluating, and improving their antiterrorism programs.)

INTRODUCTION. Criminal and terrorist acts against individuals usually occur outside the home and after the individual's habits have been established. Typically, most predictable habit is the route of travel from home to duty station or to commonly frequented local facilities.

VEHICLES

- a. Select a plain car, minimize the "rich American" look.
- b. Consider not using a government car that announces ownership.
- c. Safeguard keys.
- d. Consider carrying a cell phone in your vehicle.
- e. Auto maintenance (when turning in a vehicle for maintenance, leave only the required keys):
 - (1) Keep vehicle in good repair. You don't want it to fail when you need it most.
 - (2) Keep gas tank at least 1/2 full at all times.
 - (3) Ensure tires have sufficient tread.

PARKING

- a. Park in well lighted areas.
- b. Always lock your car...even when it's outside your house.
- c. Don't leave your car on the street overnight, if possible.
- d. Never get out without checking for suspicious persons. If in doubt, drive away.
- e. Avoid leaving keys with valet or parking attendants. If you must, leave only necessary vehicles keys.
- f. Don't allow entry to the trunk unless you're there to watch.
- g. Never leave garage doors open or unlocked.
- h. Use a remote garage door opener if available. Enter and exit your car in the security of the closed garage.

ON THE ROAD

a. Before leaving buildings to get into your vehicle, check the surrounding area to determine if anything of a suspicious nature exists. Before leaving your vehicle, look around carefully to be confident you are not headed directly into a threatening situation.

b. Before entering vehicles, check for suspicious objects on the seats. You may also look underneath the seats. Look for wires, tape or anything unusual.

c. Guard against the establishment of routines by varying times, routes, and modes of travel. Avoid late night travel.

d. Travel with companions or in convoy when possible.

e. Avoid isolated roads and dark alleys when possible.

f. Know locations of safe havens along routes of routine travel.

g. Habitually ride with seatbelts buckled, doors locked, and windows closed.

h. Do not allow your vehicle to be boxed in; maintain a minimum 8-foot interval between your vehicle and the vehicle in front; avoid the inner lanes.

i. Be alert while driving or riding.

j. Know how to react if surveillance is suspected or confirmed.

(1) Circle the block for confirmation of surveillance.

(2) Do not stop or take other actions, which could lead, to confrontation.

(3) Do not drive home.

(4) Get description of car and its occupants. Take a photograph if possible, but at a minimum, get the vehicle's license plate number.

(5) Go to nearest safehaven. Report incident to the nearest DoD counter-intelligence, security, or law enforcement organization.

k. Recognize events that can signal the start of an attack, such as:

(1) Cyclist falling in front of your car.

(2) Flagman or workman stops your car.

(3) Fake police or Government checkpoint.

(4) Disabled vehicle or accident victims on the road.

(5) Unusual detours.

(6) An accident in which your car is struck.

(7) Cars or pedestrian traffic that box you in.

(8) Sudden activity or gunfire.

1. Know what to do if under attack in a vehicle.

(1) Without subjecting yourself, passengers, or pedestrians to harm, try to draw attention to your car by sounding the horn.

(2) Put another vehicle between you and your pursuer.

(3) Execute immediate turn and escape; jump curb at 30-45-degree angle, 35 mph maximum.

(4) Ram blocking vehicle if necessary.

(5) Go to closest safe-haven.

(6) Report incident to nearest DoD counter-intelligence, security, or law enforcement organization.

COMMERCIAL BUSES, TRAINS, AND TAXIS

a. Vary mode of commercial transportation.

b. Select busy stops. Avoid standing in a group while waiting.

c. Don't always use the same taxi company.

d. Don't let someone you don't know direct you to a specific cab.

e. Ensure taxi is licensed and has safety equipment (seat belts at minimum).

(1) Ensure face of driver and picture on license are the same.

(2) Try to travel with a companion.

(3) If possible, specify the route you want taxi to follow.

(This page intentionally left blank)

AT/CIP T&R MANUAL

APPENDIX N

PERSONAL VEHICLE TIPS AND DRIVING SECURITY CHECKLIST

(This appendix is not intended to be doctrinal in nature but rather a tool for Commanders and ATOs to use when building, evaluating, and improving their antiterrorism programs.)

INTRODUCTION. An extremely important aspect of personal security is the need for regular vehicle inspections. Many terrorist actions are accomplished by placing bombs in individual vehicles. This provides the terrorist less risk and increases the chance of "hitting" the appropriate target. The following are some relatively simple steps that every driver can take to reduce the likelihood of being hurt by a terrorist act centered on a personal automobile.

VEHICLE INSPECTION TIPS

a. Every time you use your automobile, you should make a precautionary inspection. Bomb emplacement by terrorists is often rudimentary or hastily done, thereby providing the opportunity for easy detection. Make a habit of checking the vehicle and the surrounding area before entering and starting the vehicle.

(1) Check interior of the vehicle for intruders or suspicious items.

(2) Check electronic tamper device, if installed. A cheaper option is to use transparent tape on the hood, trunk, and doors to alert you to any tampering.

(3) Check underneath the car and in the fender wells for any foreign objects, loose wires, etc.

(4) Examine tires for stress marks and any evidence of tampering.

(5) Check wheel lug nuts.

(6) Check exterior for any fingerprints, smudges, or other signs of tampering.

b. You may consider the following suggestions in an effort to "harden" your vehicle:

(1) Lock the hood with an additional lock and ensure that the factory latch is located inside.

(2) Have oversized mirrors installed.

(3) Use a locking gas cap.

(4) Put two bolts through the exhaust pipe, perpendicular to one another. This prevents the insertion of explosive devices in the tail pipe.

(5) Use steel-belted radial tires.

(6) Install an intrusion alarm system and an extra battery.

(7) In high-threat areas it may be appropriate to:

(a) Install car armor.

(b) Have an interior escape latch in the trunk.

(c) Use fog lights.

(d) Install bullet resistant glass.

SUPPLEMENTAL SECURITY CHECKLIST FOR DRIVING

a. The following items are suggested procedures to be used in operating personal and government motor vehicles in areas where terrorist activity is a concern. While adhering to these practices shall not necessarily prevent a terrorist incident, continual practice and attention to detail demanded by the procedures below shall enable many potential victims to escape to safety.

b. Keep the gasoline tank of your vehicle full or near full.

c. Keep the vehicle locked at all times. Do not park on the street at night. Vehicles in locked garages should also be kept locked. Use parking lots with attendants and where the vehicle can be kept locked. Lock unattended vehicles. No matter how short the time.

d. Check up and down the street before moving out of a house and/or building into your vehicle.

e. While approaching a vehicle, check its outside for evidence of tampering. Look for wires, strings, or objects attached to or hanging from vehicle.

f. Do not touch any unusual items protruding from the vehicle, call immediately for assistance.

g. Before entering the vehicle, check the floor (front and rear) to make certain the vehicle is not occupied.

h. As you drive away from the curb, be immediately alert for surveillance of your vehicle. Look for multiple vehicle surveillance, as most attacks on vehicles have included two or more vehicles.

i. Stay alert and be prepared to take evasive actions. Keep noise level within vehicle low. Eliminate loud playing of the radio or unnecessary conversation.

j. Keep the vehicle locked while driving and the windows closed. If open, keep them rolled to within two inches of the top. This practice prevents objects from being thrown into your vehicle.

k. When possible, drive in the lane nearest the center of the roadway. This practice puts attackers at a disadvantage, avoid being boxed in. Stay in the left lane where it is difficult for pursuing vehicles to run your vehicle off the road on multi-lane highways.

l. If you encounter a roadblock manned by uniformed police or military personnel, you should stop and remain seated inside your vehicle. If asked for identification, roll the window down enough to pass your identification to the officer. Do not unlock the doors.

m. Avoid suspicious roadblocks. Do not stop. Turn and go back or turn a corner to leave the area as quickly as possible.

n. A good driver is constantly aware of possible routes of escape or evasion while behind the steering wheel.

o. In the event of a firefight between local authorities and terrorists, get down and stay low. Unless you are in the direct line of fire, it is suggested that you do not move. Experience has shown that often times anything that moves gets shot.

(This page intentionally left blank)

AT/CIP T&R MANUAL

APPENDIX O

AIR TRAVEL SECURITY TIPS

(This appendix is not intended to be doctrinal in nature but rather a tool for Commanders and ATOs to use when building, evaluating, and improving their antiterrorism programs.)

INTRODUCTION. Air travel, particularly through high-risk airports or countries, poses security problems different from those of ground transportation. Here are some simple precautions that can reduce vulnerabilities of a terrorist assault.

MAKING TRAVEL ARRANGEMENTS

- a. Use office symbols on orders or leave authorizations if the word description denotes a high or sensitive position.
- b. Get an AOR specific threat briefing from your security officer, antiterrorism officer, or the appropriate counter-intelligence or security organization prior to overseas. This briefing is required prior to travel overseas and must occur within three months of travel.
- c. Before traveling, consult the DoD Foreign Clearance Guide (available at www.fcgi.pentagon.mil) (reference (ay)) to ensure you know and can meet all requirements for travel to a particular country.
- d. Use military air, USTRANSCOM/AMC military contract, or U.S. flag carriers if available and consistent with mission requirements.
- e. Avoid scheduling through high-risk areas. If necessary, use foreign flag airlines and/or indirect routes to avoid high-risk airports.
- f. Don't use rank or military address on tickets, travel documents, or hotel reservations.
- g. Seats in the center of the aircraft tend to offer the greatest protection since they are farther from the usual center of hostile action, which is most often near the cockpit or terrorists at the rear of the aircraft.
- h. Seats at an emergency exit may provide an opportunity to escape.
- i. When available, use government quarters or contracted hotels as opposed to privately arranged off-base hotels.

PERSONAL IDENTIFICATION

- a. Don't discuss your military affiliation with anyone.
- b. Maintain unofficial form (s) of identification (tourist passport and/or driving license) to show airline and immigration officials as required.

c. Carry only limited DoD documentation on one's person (keep discreet). If you must carry these documents on your person, select a hiding place on board the aircraft in case of a hijacking. Don't carry classified documents unless they are absolutely mission-essential.

d. Consider use of a tourist passport, if you have one, with necessary visas, providing it's allowed by the country you are visiting.

LUGGAGE

a. Use plain, civilian luggage; avoid military looking bags, B-4 bags, duffel bags, etc.

b. Remove all military patches, logos, or decals from your luggage and briefcase.

c. Ensure luggage tags don't show your rank or military address.

d. Don't carry official papers in your briefcase.

CLOTHING

a. Travel in conservative civilian clothing when using commercial transportation or when traveling military airlift if you have to connect with a flight at a commercial terminal in a high-risk area.

b. Don't wear distinct military items such as organizational shirts, caps, or military issue shoes or glasses.

c. Don't wear U.S. identified items such as cowboy hats or boots, baseball caps, American logo T-shirts, jackets, or sweatshirts.

d. Wear a long-sleeved shirt or bandage if you have a visible U.S. affiliated tattoo.

PRECAUTIONS AT THE AIRPORT

a. Arrive early; watch for suspicious activity.

b. Look for nervous passengers who maintain eye contact with others from a distance. Observe what people are carrying. Note behavior not consistent with that of others in the area.

c. No matter where you are in the terminal, identify objects suitable for cover in the event of attack. Pillars, trash cans, luggage, large planters, counters, and furniture can provide protection.

d. Don't linger near open public areas. Proceed through security checkpoints as soon as possible in order to be in a more secure area.

e. Be extremely observant of personal carry-on luggage. Thefts of briefcases designed for laptop computers are increasing at airports worldwide. Likewise, luggage not properly guarded provides an opportunity for a terrorist to place an unwanted object or device in your carry-on bag. As much as possible, do not pack anything you cannot afford to lose; if the documents are important, make a copy and carry the copy.

- f. Avoid secluded areas that provide concealment for attackers.
- g. Be aware of unattended baggage anywhere in the terminal.
- h. Observe the baggage claim area from a distance. Do not retrieve your bags until the crowd clears. Proceed to customs lines at the edge of the crowd.
- i. Report suspicious activity to airport security personnel.
- j. Proceed through security checkpoints as soon as possible.
- k. Be extremely observant of personal carry-on luggage.

ACTIONS IF ATTACKED IN AN AIRPORT

- a. If being attacked by bomb or grenade, dive for cover. Do not run; running increases the probability of shrapnel hitting vital organs or the head.
- b. If you must move, belly crawl or roll. Stay low to the ground, using available cover.
- c. If you see grenades, seek immediate cover, lay flat on the floor, feet and knees tightly together with soles toward the grenade. In this position, your shoes, feet, and legs protect the rest of your body. Shrapnel shall rise in a cone from the point of detonation, passing over your body.
- d. Place arms and elbows next to your ribcage to protect your lungs, heart, and chest. Cover your ears and head with your hands to protect neck, arteries, ears, and skull.
- e. The responding security personnel shall not be able to distinguish you from attackers. Do not attempt to assist them in any way. Lay still until told to get up.

AIRPLANE HIJACKINGS

- a. Determining the best response in a hostage situation is a critical judgment call. Passengers need to remain extremely alert and rational to try to understand the intentions of the hijackers. Sitting quietly may be prudent in most circumstances, but it is conceivable the situation may require actions to prevent hijackers from taking control of the aircraft. In all situations, it is important for individuals to remain alert to unexpected events, think clearly, and act responsibly. If hijackers are flying the plane, a suicide attack with the aircraft is highly probable, and a coordinated attack by the passengers may be appropriate.
- b. Remain calm, be polite and cooperate with your captors.
- c. Be aware that all hijackers may not reveal themselves at the same time. A lone hijacker may be used to draw out security personnel for neutralization by other hijackers.
- d. Surrender your tourist passport in response to a general demand for identification.

e. Don't offer any information; confirm your military status if directly confronted with the fact. Be prepared to explain that you always travel on your personal passport and that no deceit was intended.

f. Discreetly dispose of any military or U.S. affiliated documents.

g. Don't draw attention to yourself with sudden body movements, verbal remarks, or hostile looks.

h. Prepare yourself for possible verbal and physical abuse, and lack of food, drink, and sanitary conditions.

i. If permitted, read, sleep, or write to occupy your time.

j. Discreetly observe your captors and memorize their physical descriptions. Include voice patterns and language distinctions, as well as clothing and unique physical characteristics. Observe how heavily they're armed.

k. If possible, observe if the pilots remain in control of the aircraft.

l. Be aware there may be Federal authorities, such as Air Marshals, on the aircraft that may be best suited to take action.

m. Cooperate with any rescue attempt. Remain still and follow instructions of rescuers. If possible, lie on the floor until told to rise.

AT/CIP T&R MANUAL

APPENDIX P

USE OF PROTECTIVE SECURITY DETAILS

(This appendix is not intended to be doctrinal in nature but rather a tool for Commanders and ATOs to use when building, evaluating, and improving their antiterrorism programs.)

INTRODUCTION

a. The use of Protective Security Details (PSDs) is a policy decision. There are pros and cons to their use. The employment of large numbers of PSD members to protect a few senior officers or DoD officials may deter all but the most determined terrorist attack. On the other hand, the use of one or two PSD members may attract attention to the protected person that might otherwise not be given to that individual.

b. DoD personnel can be their own bodyguards if they follow the self-protection strategy outlined in this handbook. Supplemented by a chauffeur trained in defensive driving and other security techniques, DoD executives should be relatively safe in most situations.

c. In high crisis situations, in areas where kidnapping is rampant, and during period of direct threats, use of PSDs for high-risk personnel should be strongly considered.

d. It is critical that members of PSDs be thoroughly trained to do their job. PSD training is intensive and cannot be done overnight, nor can individuals who have been trained retain levels of proficiency in driving, firearms, and close combat without continuous training. The PSD members must be physically and mentally fit so that their bodies and minds shall respond positively in crisis situations.

e. Since PSD members must both protect protectees and be their companions in personal and professional situations they must be particularly honest and discrete.

f. The training of bodyguards should begin by defining their role -- both as a technical aid to the executive they serve and as an individual who can direct the executive they protect to self-help. In an attack, PSD members may be killed or incapacitated. In their protective roles, PSD members should be constantly teaching protectees to protect themselves, to avoid attack, to respond to an attack, and to conduct themselves properly if captured.

PSD MEMBER TRAINING OBJECTIVES

a. Members of PSDs should be instructed in the following areas:

- (1) History of threats from criminals and terrorists.
- (2) Assassinations/executions.
- (3) Kidnap/hostage/ransom actions.

(4) Extortion actions.

b. Destruction of Government and Government-related facilities. The psychology of criminals and extremists.

c. It is particularly important that the general instruction received as part of the general and professional military training of PSD members be supplemented by local information. Such information should emphasize terrorist activity in the area of operations where PSD members are to provide protection to senior officers and DoD officials.

TARGET CHARACTERISTICS

a. In developing a strategy for the use of PSD members to provide additional protection, it is essential that protectees examine their personal roles, missions, functions, and lifestyles to assess their individual and dependents risk and vulnerability to terrorist attack. The following considerations should be weighed in developing a PSD protective plan:

(1) Official Role. PSDs should be assigned to high-risk personnel based on their duties, responsibilities, risk, vulnerability, and importance or criticality to DoD missions and functions. The following questions should be considered in determining the need for assignment PSD to senior officers or DoD officials.

(2) What is the public profile of the officer or DoD official? What is DoD, Combatant Command, or Embassy protection policy?

(a) What are the strengths and weaknesses of the physical security system?

(3) What are local DoD or Embassy security procedures?

(4) What coordination occurs between local (host nation) law enforcement officials and U.S. Government, the Department of Defense, or Embassy security personnel?

b. How close are relations between the U.S. Government and the state, municipal, local or foreign host Government?

c. How much (quantity and quality) information on potential threats is being provided from all sources? How fast does this information arrive; how fast is it assessed, and how fast can it be disseminated for those with need to know?

(1) The Protectee. In developing a plan for the protection of senior officers, DoD officials, and their dependents, the following personal characteristics, interests, and lifestyle considerations should be weighed:

(a) The executive and his family.

(b) Public and private profile.

(c) Politics and psychology.

(d) Zones of vulnerability.

(e) Executive.

1. Residence.
 2. Movement.
 3. Work.
 4. Social functions.
 5. Recreation.
- (f) Family.
1. Residence.
 2. Movement.
 3. Shopping and/or school.
 4. Social functions.
 5. Recreation.

PSD MEMBERS AND THEIR RESPONSIBILITIES

a. Relationship to Executive PSD members may be asked to perform a wide variety of tasks in the context of providing additional security protection to senior officers and DoD officials. Protective services may be provided from the following positions or functions:

- (1) At fixed post.
- staff.
- (a) Need for secrecy, monitoring children, monitoring domestic
 - (b) Observation and/or surveillance.
 - (c) Monitoring phone, mail, etc.
 - (d) Monitoring pattern avoidance.
 - (e) Emergency plans: fire, bomb threat, natural disaster, escape, threat notification, evacuation.
 - (f) Penetration tests.
 - (g) Dogs.
 - (h) Lighting.
 - (i) Alarm systems.
 - (j) Weapons.
 - (k) Security surveys and implementation.
 - (l) Concealed personal survival equipment.
 - (m) Hideouts/protected locations/safe rooms.

- (n) What to do until help arrives.
 - (o) Emergency communications and response.
 - (p) Attacker confusion and neutralization devices and techniques.
 - (q) The family emergency plan.
- (2) As driver.
- (a) What to expect from attacker.
 - (b) Vulnerability through pattern development.
 - (c) Element of surprise.
 - (d) Single vehicle cutoff.
 - (e) Two vehicle cutoff.
 - (f) Road blocks.
 - (g) How to respond (Protected vehicles: escorted, unescorted).
 - (h) Selection of vehicle and security modifications.
 - (i) Horsepower/body style.
 - (j) Tires.
 - (k) Mirrors.
 - (l) Glass.
 - (m) Concealed weapons.
 - (n) Armor.
 - (o) Lights.
 - (p) Noise and/or sirens.
 - (q) Communications.
 - (r) Defensive Driving.
 - (s) Alertness and observation.
 - (t) Drive ahead and plan ahead.
 - (u) Pattern avoidance.
 - (v) Neutralizing forms of attack.
 - (w) Escape routes and safe havens.
 - (x) Locked car as barrier.

- (y) Defensive driving techniques.
- (z) Chemical irritants.
- (aa) First aid.
- (bb) Coping with fire.
- (cc) Bomb recognition and handling.
- (dd) Photography
- (3) As all around bodyguard.
- (4) Discipline.
- (5) Conduct.

(a) PSD members must be skilled in negotiation with protectees, their families, their colleagues, and their acquaintances over the proper balance between security considerations on the one hand, and family, social, and business activities on the other. They must retain their composure at all times, even if protectees and those around them do not, especially over matters of appropriate security arrangements for home, official business away from the office, and recreational activities.

(b) PSD members must also be skilled in remaining focused on the need for protection, regardless of the behaviors or personal practices of protectees. In addition, PSD members shall have an opportunity to observe senior officers, DoD officials, and their families in close, personal situations. As there are often significant differences between public and private personalities, PSD members may be placed in positions where their ideals, personal values, expectations, and preferences differ significantly from the person or people they are protecting.

(c) PSD members must be prepared to perform other duties as may be required to preserve their anonymity on the one hand, and the anonymity of the protectee on the other. If a protectee is scheduled to attend a meeting for which a secretary might be used to take notes, a member of the PSD team may be assigned the task of note taking, thereby keeping the size of the protectee's entourage small. By performing secretarial duties in connection with a PSD assignment, the PSD member does not reveal his or her special training to outside observers. In addition, he or she does not reveal U.S. Government concerns about the risk or vulnerability of the protected person to a terrorist attack.

(6) Appearance.

(a) PSD members must appear to be part of their protectees entourage. They must "fit in" with the protectee's functions, roles, and lifestyles. As noted above, they may be asked to perform other duties not directly related to security in order to disguise their primary security duties.

(b) PSD members should dress, groom, and act as part of the protectee's environment. Consider longer hairstyles, functional jewelry, low-key manicures, and even civilian attire for PSD members assigned to

senior DoD officials. Consider more mature members of PSD details for assignment to senior officers as "aides" or "assistants" as well as younger members of PSDs as drivers and couriers.

(7) Organizational Security Plans and Contingencies.

(a) PSD members need to be kept informed of physical security and personnel security arrangements as they develop and change. It is essential that PSDs know the location of response forces and backup response forces, the communications links to reach such forces, communication links with local, municipal, and host country security resources (as necessary). PSD members should be given detailed information on the location of safe havens, pre-surveyed evacuation sites, pre-surveyed evacuation routes, and identified backup or alternatives.

(b) PSD members should be invited to observe and to participate in crisis management training and exercises so that they can appreciate the roles and responsibilities of their protectees and identify positions from which they can continue to perform their responsibilities without interfering with other members of the crisis management team.

(c) Tools and Techniques. PSD members bring a wide range of "tools" and "techniques" to their responsibilities of protecting senior officers and DoD officials. At the same time, protectees and their organizations need to be sensitive to some of the requirements or special considerations that PSDs may have in order to carry out their assignments. The following are some, but perhaps not all, of the considerations PSDs and host organizations need to examine.

WHAT PSD MEMBERS MUST TEACH PROTECTEES

a. PSD members and their protectees must jointly develop routines to detect, classify, assess, and respond to threats to the protectees security. The following issues must be addressed and plans jointly developed and practiced.

- (1) Duress signals.
- (2) Call-in.
- (3) Carrying duress notes written on money.
- (4) Duress alarms and/or radio links.
- (5) Varying routines.
- (6) Clothing changes.
- (7) Mutual observation.
- (8) Contact with police.
- (9) Hazards of swimming, fishing, boating, etc.
- (10) What to do if taken captive.
- (11) Cooperate and stay calm.

(12) Avoidance of psychological link with kidnappers.

(13) Prepared stories.

(14) Use of codes.

(15) Verbal contact.

(16) Concealed aids.

b. These considerations must be discussed jointly because the protectee and PSD members shall be much more likely to remember during an emergency those plans and procedures jointly developed. Practice of these plans should occur on a continuing basis, especially during periods of high threat.

(This page intentionally left blank)

AT/CIP T&R MANUAL

APPENDIX Q

SPECIFIC CONSTRUCTION PROTECTIVE MEASURES

(This appendix is not intended to be doctrinal in nature but rather a tool for Commanders and ATOs to use when building, evaluating, and improving their antiterrorism programs.)

SPECIFIC CONSTRUCTION PROTECTIVE MEASURES. This enclosure discusses general construction protective measures. Combatant Commanders, Service and/or local commands provide specific guidance for unique/site-specific standards. While there are many ways to organize the variety of possible construction protective measures available to specific installations, one way to do so generally aligns with the seven previously discussed construction design strategies. Specific measures and other construction considerations generally fall within the four groupings of site planning, structural design, architectural design, and electrical and mechanical design. Other construction terms such as landscape design, parking security, interior design, fire protection engineering, and electronic security are generally addressed within these four groupings. Specific measures and other construction considerations are provided below.

SITE PLANNING

a. Operational, logistics, and security requirements should be integrated in the overall design of buildings, equipment, landscaping, parking, roads, and other features. If implemented, the following additional measures, as well as related creative solutions developed during this phase, can significantly enhance site security with little increase in cost and should be considered for all inhabited buildings.

b. Building Location Considerations

(1) Standoff and Building Separation Distances. Maximize where practical, meeting the DoD AT minimum standoff distances and specific combatant command guidance at locations without specific threat, but mitigate possible blast effects when required standoff distances cannot be met or higher threats exist than the structure is capable of protecting occupants. Other key concepts relating to standoff and building separation distances are controlled perimeter, parking and roadways, family housing, and trash receptacles.

(2) Vantage Points. Vantage points are natural or man-made positions from which potential aggressors can observe and target people or other assets in and around a building. Identify vantage points outside the control of personnel in the targeted building and either eliminate them or provide means to avoid exposure to them. Means to avoid exposure may include actions such as reorienting the building or shielding people or assets in and around the building using such measures as reflective glazing, walls, privacy fencing, or vegetation.

(3) Visitor Populations. Activities with large visitor populations provide opportunities for potential aggressors to get near buildings with minimal controls and therefore limit opportunities for early detection.

Maximize separation distance between inhabited buildings and areas with large non-DoD visitor populations.

(4) Commercial Transportation Nodes. Avoid sites for inhabited buildings that are close to railroads, ports, airfields, and major road networks. Where any of these transportation nodes are in the vicinity of existing buildings, provide adequate standoff distances from inhabited buildings required to controlled perimeters. Where those standoff distances are not available and since moving things (such as existing railroads) may be difficult and prohibitively expensive, ensure that there are procedures in place to prohibit trains or other similar transportation vessels from stopping in the vicinity of inhabited structures.

(5) Unobstructed space. Aggressors will not generally place assets in areas near buildings where their explosive devices could be visually detected by building occupants observing the area around the building. Obstructions within 10 meters (33 feet) of buildings should not be permitted that allow for concealment from observation of explosive devices 150 mm (six inches) or greater in height. This does not preclude the placement of site furnishings or plantings around buildings. It only requires conditions such that any explosive devices placed in that space would be observable by building occupants. Unobstructed space also addresses electrical and mechanical equipment, and equipment enclosures to eliminate opportunities for placement and concealment of explosive devices.

c. Vehicle Considerations

(1) Vehicle Access. The first line of defense in limiting opportunities for aggressors to get vehicles close to DoD buildings is at vehicle access points at the controlled perimeter, to parking areas, and at drive-up/drop-off points. Keep the number of access points to the minimum necessary for operational or life safety purposes. That will limit the number of points at which access may have to be controlled with barriers and/or personnel in increased threat environments or if the threat increases in the future.

(2) High-speed vehicle approaches. The energy of a moving vehicle increases with the square of its velocity; therefore, minimizing a vehicle's speed allows vehicle barriers to be lighter and less expensive should vehicle barriers ever become necessary. To facilitate reductions in vehicle speeds in the future, ensure there are no unobstructed vehicle approaches perpendicular to perimeters at the required parking and roadway standoff distances.

(3) Drive-up/drop-off and access roads. Some facilities require access to areas within the required standoff distance for dropping off or picking up people or loading or unloading packages and other objects. Examples that may require drive-up/ drop off include, but are not limited to, medical facilities, exchanges and commissaries, childcare centers, and schools. Here consideration is given to marking, unattended vehicles, access control and location of the drive-up/drop-off and access roads to prevent unauthorized vehicles from being parked and left unattended or located under any inhabited portion of a building. Additionally, locate these points away from large glazed areas of the building to minimize the potential for hazardous flying glass fragments in the event of an explosion. The drive-up/drop-off point should be coordinated with the building geometry to

minimize the possibility that explosive blast forces could be increased due to being trapped or otherwise concentrated.

(4) Parking beneath buildings. Parking beneath buildings makes building occupants highly vulnerable and this parking should be eliminated where possible. Where very limited real estate makes parking beneath buildings unavoidable, the following measures should be incorporated into the design for new buildings or mitigating measures should be incorporated into existing buildings to achieve an equivalent level of protection. Ensure that access at personnel and vehicle entrances to parking areas is physically controlled, that the floors beneath inhabited areas will not breach from a detonation in the parking area, and that all structural elements within and adjacent to the parking area will be subject to the progressive collapse provisions.

(5) Entry control points for family housing. For new family housing areas, provide space for an entry control point at the perimeter of the housing area so that a controlled perimeter can be established there if the need arises in the future.

STRUCTURAL DESIGN

a. If adequate standoff distances are achieved, conventional construction provides some protection from a terrorist attack. However, even when standoff distances exist, additional structural measures should be incorporated into building designs to ensure that buildings do not sustain damage disproportionate to the original localized damage, collapse, or create hazardous debris.

b. Progressive collapse avoidance. Progressive collapse is considered to be significant risk for buildings of three stories (not including basement stories) or more. The superstructure can be designed to sustain local damage with the structural system as a whole remaining stable and not being damaged to an extent disproportionate to the original local damage. An arrangement of the structural elements can provide stability to the entire structural system by transferring loads from any locally damaged region to adjacent regions capable of resisting those loads without collapse. This shall be accomplished by providing sufficient continuity, redundancy, or energy dissipating capacity (ductility), or a combination thereof, in the members and connections of the structure. To verify the design a structure must be analyzed in a number of ways. Additionally, all floors need improved capacity to withstand load reversals (caused by blast effects) by designing them to withstand a net uplift at least equal to the dead load plus one-half the live load. For example, some existing buildings have been outfitted with steel beam systems to reinforce the existing structure to provide an appropriate level of protection.

c. Exterior walls. A significant number of DoD buildings have un-reinforced masonry exterior walls that would likely crumble with a fairly small explosive without adequate standoff. As a result, with inadequate standoff, un-reinforced masonry walls should be prohibited for the exterior walls of inhabited buildings. Buildings should have adequate reinforcement of at least a minimum of 0.05 percent vertical reinforcement with a maximum spacing of 1200 mm (48 in) or have mitigating measures to provide an equivalent level of protection. There are many available ways to reinforce exterior walls to provide adequate protection for building occupants.

d. Structural isolation. Where there are areas of buildings that do not meet the criteria for inhabited buildings, design the superstructures of those areas to be structurally independent from the inhabited area. This will minimize the possibility that collapse of the uninhabited areas of the building will affect the stability of the superstructure of the inhabited portion of the building. Alternatively, verify through analysis that collapse of uninhabited portions of the building will not result in collapse of any portion of the building.

e. Building overhangs. Avoid building overhangs with inhabited spaces above them where people could gain access to the area underneath the overhang. Where such overhangs must be used, measures should be incorporated into the design for new buildings or mitigating measures should be incorporated into existing buildings to achieve an equivalent level of protection so that roadways and/or parking areas are not under overhangs, that floors beneath inhabited areas will not breach from the detonation underneath the overhang, and that all structural elements within and adjacent to the overhang will not suffer progressive collapse.

ARCHITECTURAL DESIGN

a. There are many aspects of building layout and other architectural design issues that significantly enhance building occupant' safety and security with little increase in cost and should be fully explored and leveraged for all inhabited buildings.

b. Windows and glazed doors. To minimize hazards from flying glass fragments, glazing and window frames are key components for all inhabited buildings. Windows and frames should work as a system to ensure that their hazard mitigation is effective and apply even if adequate standoff distances are met. Specific measures are available to further mitigate glazing and window frames hazards where standoff distances are not met. Additionally, whenever window or door glazing is being replaced in existing inhabited buildings as part of a planned renovation, it should meet the same guidelines.

c. Building access. The areas outside of installations are commonly not under the direct control of the installations. People entering and exiting the buildings are vulnerable to being fired upon from vantage points (discussed in site planning) outside the installations

(1) Main entrance. To mitigate those vulnerabilities in new buildings ensure that the main entrance to the building does not face an installation perimeter or other uncontrolled vantage points with direct lines of sight to the entrance. For existing inhabited buildings where the main entrance faces an installation perimeter either use a different entrance as the main entrance or screen that entrance to limit the ability of potential aggressors to target people entering and leaving the building.

(2) Exterior doors. For all new and existing buildings, ensure that all exterior doors into inhabited areas open outwards. By doing so the doors will seat into the doorframes in response to an explosive blast, increasing the likelihood that the doors will not enter the buildings as hazardous debris.

(3) Internal circulation. Design circulation within buildings to provide visual detection and monitoring of unauthorized personnel approaching controlled areas or occupied spaces.

(4) Asset location. To minimize exposure to visual detection, monitoring, direct blast effects and potential impacts from hazardous glass fragments and other potential debris, consider placement of key personnel, critical assets, to minimize risk.

(a) Critical assets and mission critical or high-risk personnel. Locate away from the building exterior.

(b) Visitor control. Controlling visitor access points maximizes the possibility of detecting potential threatening activities. Keep visitor control points in buildings away from sensitive or critical areas, areas where high risk or mission critical personnel are located, or other areas with large population densities of DoD personnel.

(c) Room layout. In rooms adjacent to the exterior of the building position personnel and critical equipment to minimize exposure to direct blast effects and potential impacts from hazardous glass fragments and other potential debris.

(d) External hallways. Because doors can become hazardous debris during explosive blast events, because doors designed to resist blast effects are expensive, and because external hallways have large numbers of doors leading into inhabited areas, avoid exterior hallway configurations for inhabited structures.

(e) Mailrooms. As mail bombs are frequent methods employed by terrorists, protective measures need to address the location of rooms to which mail is delivered or in which mail is handled in inhabited buildings. The measures involve limiting collateral damage and injuries and facilitating future upgrades to enhance protection should they become necessary. By locating the mailroom on the building perimeter there is an opportunity to modify it in the future if a mail bomb threat is identified. Where mailrooms are located in the interior of buildings, few retrofit options are available for mitigating the mail bomb threat. Mailrooms should also be located as far from heavily populated areas of the building and critical infrastructure as possible. This measure will go far toward minimizing injuries and damage if a mail bomb detonates in the mailroom where the mailroom is not specifically designed to resist that threat.

d. Roof access. For all inhabited buildings, control access to roofs to minimize the possibility of aggressors placing explosives or chemical, biological, or radiological agents there or otherwise threatening building occupants or critical infrastructure. For new buildings eliminate all external roof access by providing access from internal stairways or ladders, such as in mechanical rooms. For existing buildings eliminate external access where possible, or secure external ladders or stairways with locked cages or similar mechanisms.

e. Overhead mounted architectural features. For all buildings, ensure that all suspended ceiling systems and other overhead mounted architectural features are mounted to minimize the likelihood that they will fall and injure building occupants. For example, in the DoD AT construction standards, all such systems will be mounted such that they resist forces of 0.5 times the component weight in any direction and 1.5 times the component

weight in the downward direction. But this standard does not preclude the need to design architectural feature mountings for forces required by other criteria such as seismic standards.

f. Minimize secondary debris. Eliminate un-revetted concrete barriers and site furnishings in the vicinity of inhabited structures that are accessible to vehicle traffic. Revet exposed concrete surfaces with 1 meter (3 feet) of soil to prevent fragmentation hazards in the event of an explosion.

ELECTRICAL AND MECHANICAL DESIGN

a. Electrical and mechanical design standards address limiting damage to critical infrastructure, protecting building occupants against chemical, biological, and radiological threats, and notification of building occupants of threats or hazards.

b. HVAC

(1) Air intakes. Air intakes to HVAC systems that are designed to move air throughout a building that are at ground level provide an opportunity for aggressors to easily place contaminants that could be drawn into the building. For all new inhabited buildings locate all air intakes at least 3 meters (10-ft) above the ground and is recommended for existing inhabited buildings.

(2) Emergency air distribution shutoff. All buildings should provide an emergency shutoff switch in the HVAC control system that can immediately shut down air distribution throughout the building. The switch (or switches) should be located to be easily accessible by building occupants. Providing such a capability will allow building occupants to limit the distribution of airborne contaminants that may be introduced into the building.

c. Utility distribution and installation. Utility systems can suffer significant damage when subjected to the shock of an explosion. Some of these utilities may be critical to safely evacuating personnel from the building or their destruction could cause damage that is disproportionate to other building damage resulting from an explosion. Where possible, route critical or fragile utilities such that they are not on exterior walls or on walls shared with mailrooms to minimize the possibility of the above hazards. Where redundant utilities are required in accordance with other requirements or criteria, ensure that the redundant utilities are not collocated or do not run in the same chases. This minimizes the possibility that both sets of utilities will be adversely affected by a single event.

d. Equipment bracing. Mount all overhead utilities and other fixtures to minimize the likelihood that they will fall and injure building occupants. For example, DoD AT construction standards require all equipment mountings to be designed to resist forces of 0.5 times the equipment weight in any direction and 1.5 times the equipment weight in the downward direction. But they do not preclude the need to design equipment mountings for forces required by other criteria such as seismic standards.

e. Under building access. To limit opportunities for aggressors placing explosives underneath buildings ensure that access to crawl spaces, utility tunnels, and other means of under building access is controlled.

f. Mass notification. All inhabited buildings should have a timely means to notify occupants of threats and instruct them what to do in response to those threats. The capability enables real-time information to be provided to building occupants or personnel in the immediate vicinity of the building during emergency situations. The information relayed should be specific enough to discriminate appropriate response actions. Any system, procedure, or combination thereof that provides this capability will be acceptable.

(This page intentionally left blank)

AT/CIP T&R MANUAL

APPENDIX R

MAIL HANDLING SUSPICIOUS PACKAGES

(This appendix is not intended to be doctrinal in nature but rather a tool for Commanders and ATOs to use when building, evaluating, and improving their anti-terrorism programs.)

INTRODUCTION. AP19.1.1. This Appendix offers information to assist personnel in identifying suspicious envelopes and packages and actions to take in the event hazardous or explosive content is detected. Although thorough, the list below identifies typical indicators and personnel should remain vigilant for not-so-typical indicators. If a suspicious envelope or parcel is located, personnel should perform the actions listed at the end of this Appendix.

INDICATORS OF SUSPICIOUS ENVELOPES AND PARCELS

a. The following are typical indicators that highlight suspicious envelopes and parcels.

(1) Unknown or strange postmark. The mail may be postmarked from a strange or unknown place, usually outside your normal channels of correspondence.

(2) Lack of return address. This may be an attempt by the terrorist to reduce the amount of evidence on an envelope or to avoid suspicion by using what could be determined to be an erroneous address.

(3) Excessive amount of postage. It is risky to ask a mail clerk to weigh a letter bomb for the exact amount of postage. Postal personnel normally know what to look for and may be able to determine that the package contains a bomb. Therefore, it is safer for the terrorist to add additional postage rather than risk being caught with the bomb.

(4) Abnormal or unusual size or shape. The envelope or package may be of an abnormal, excessive, or unusual size because of the construction of the firing device and other bomb parts inside.

(5) Protruding strings, aluminum foil, or wires. Strings or wires may protrude from or be attached to the item. The bomb maker may have constructed the device in a sloppy manner, causing unsecured wires to work loose. The more likely reason for an exposed wire is that it is an arming wire that the courier did not remove, fearing it would detonate instantaneously.

(6) Misspelled words. Misspelling on the envelope or package could occur because the writer is simply not familiar with military ranks or unit designations.

(7) Inconsistency between the return address and the postmark. The return address and the postmark may be different; e.g., the return address may indicate the item was mailed from Oregon, whereas the postmark may indicate Frankfurt, Germany.

(8) Handwritten labels, foreign handwriting, or poorly typed addresses. Handwriting that appears to be foreign may indicate that the bomber, or whoever addressed the item, is from another country.

(9) Unusual odor. The item may exhibit an unusual odor, such as shoe polish, almonds, or marzipan (a sweet almond paste used predominately in Germany for candies). Heavily perfumed packages or envelopes may also indicate a device is present. NOTE: Intentionally smelling an envelope or package to determine existence of an unusual odor is not advised. Deliberate smelling of envelopes and packages may expose personnel to chemical or biological agents. The intent of this indicator is that unusual odors may be detected under normal operating conditions and without close scrutiny.

(10) Unusual weight. The item may be unusually heavy or light for its size. A normal envelope weighs 1 to 2 ounces, compared to a letter bomb, measuring one-fourth to one-half inch thick. It may appear to contain a small report or pamphlet rather than a few sheets of paper. A package may be unusually light if it contains only the firing device, power source, and explosive, rather than whatever is listed on the exterior of the package, such as books or other materials.

(11) Unbalanced weight. The balance of the item may be uneven because of the way the explosives are placed or because they have shifted to one side.

(12) Springiness in the top, bottoms, or sides. This may result from the bomb having a pressure-release-type switch. Also, the wires used to construct the device may cause the springiness.

(13) Inflexibility. The envelope may be inflexible if the firing device and other contents have been mounted on material to prevent shifting around while traveling through the mail system. If the internal components have simply been glued or mounted to the sheet explosive, the envelope may stay in a flexed or semi-flexed position when bent.

(14) Crease marks, discoloration, or stains. Crease marks or stains, such as those from potato chips or French fries, may show on the outside. This happens because many explosives sweat or exude the oil used in their manufacture, such as motor (Semtex-H) or vegetable (C-4) oil.

(15) Incorrect titles or title but no name. Often, suspect envelopes or packages are addressed to figureheads, such as "Commander" or "Director" and not "Colonel Jones" or "Mr. Smith."

(16) Excessive security material, such as masking tape, string, etc. To prevent inadvertent compromise of package contents, excessive security material is used to ensure package integrity during transit.

(17) Ticking, beeping, or other sounds. Seldom used, analog timers are still a possibility. Digital timers may emit faint beeps or other sounds.

(18) Marked with restrictive endorsements, such as "Personal," "Rush, Do Not Delay," or "Confidential." Restrictive endorsements ensure suspect envelope or package is opened only by the target individual.

(19) Evidence of powder or other contaminants. Chemical or biological contaminants can escape through envelope or package seams.

PREVENTATIVE MEASURES

a. To minimize exposure to chemical or biological-laden envelopes and packages, mail handlers should use gloves when handling mail and have several large sealable bags nearby for isolating suspicious mail and discarding all clothing worn when in contact with a suspicious parcel. Surgical masks or protective masks and a change of clothing should also be kept in mailrooms. Powder coated gloves should be avoided as the powder may be associated with a chemical or biological contamination from the mail.

b. Commanders should be aware that individual protective masks are commercially available which provide a significant level of protection against inhalation of certain biological agents. High Efficiency Particulate Air filter masks are relatively inexpensive, available, and effective. Discretionary use is advisable to mitigate risk of exposure.

c. Personnel should be instructed on the location, security procedures, and process for disabling building ventilation systems.

ACTIONS TO TAKE UPON ENCOUNTERING A SUSPICIOUS ENVELOPE OR PACKAGE

a. Personnel, upon encountering a suspicious envelope or package, should follow these suggested actions:

(1) DO NOT PANIC.

(2) For a suspicious unopened envelope or package, perhaps marked with a threatening message:

(a) Do not open the envelope or package.

(b) Do not shake or empty the contents of any suspicious envelope or package.

(c) Place the envelope or package in a plastic bag or some other type of container to prevent leakage of contents. If you do not have any container, cover the envelope/package using clothing, paper, a trashcan, etc., and do not disturb this cover.

(d) Evacuate the room, close the door, and secure the area to prevent further access.

(e) If handling envelopes or packages suspected of containing chemical or biological contaminants, wash hands with soap and water to prevent potential of spreading any powder or contaminant.

(f) If at home, dial the local emergency number, such as "9-1-1," and report the incident to local police. If at work, report the incident to local police, chain of command personnel, and the building security manager. If warranted, contact the local FBI field office.

(g) Make a list of all people who were in the room or area when the suspicious envelope or package was recognized. Public health authorities

and law enforcement officials may need this information for follow-up advice and investigations.

(3) For an envelope or package containing powder or other contaminant that spills out onto a surface:

(a) Avoid inhalation of the contaminant. Don respiratory protection if available.

(b) Do not try to clean up the contaminant. Immediately and carefully cover the envelope or package and spilled contents using clothing, paper, a trashcan, etc., and do not disturb this cover.

(c) Evacuate the room, close the door, and secure area to prevent further access.

(d) Wash your hands with soap and water to prevent potential of spreading contaminant.

(e) If at home, dial the local emergency number, such as "9-1-1," and report the incident to local police. If at work, report the incident to local police, chain of command personnel, and the building security manager. If warranted, contact the local FBI field office.

(f) Remove contaminated clothing as soon as possible and place in a plastic bag or other container capable of being sealed. The sealed clothing should be given to emergency responders for proper handling.

(g) Shower with soap and water as soon as possible. Do not use bleach or other disinfectant on skin. The intent is to flush the contaminant from the skin; excess scrubbing or brushing may cause abrasions allowing the contaminant to penetrate the skin.

(h) Make a list of all people who were in the room or area when the suspicious envelope or package was recognized, especially those who had actual contact with the contents. Public health authorities and law enforcement officials may need this information for follow-up advice and investigations.

(4) If there is a question of room or air handling system contamination by aerosolized agents:

(a) If possible, disable ventilation unit/fans in the local area.

(b) Evacuate the area immediately, close the door, and secure area to prevent further access.

(c) If at home, dial the local emergency number, such as "9-1-1," and report the incident to local police. If at work, report the incident to local police, chain of command personnel, and the building security manager. If warranted, contact the local FBI field office.

(d) Shut down air handling system if possible.

(e) Make a list of all people who were in the room or area. Public health authorities and law enforcement officials may need this information for follow-up advice and investigations.

AT/CIP T&R MANUAL

APPENDIX S

ABBREVIATIONS AND ACRONYMS

The following abbreviations are used in this Training and Readiness Manual:

AAR After Action Review

ACIC Army Counterintelligence Center

AFOSI U.S. Air Force Office of Special Investigation

AM Attack Means

AMC Air Mobility Command

AOR Area of Responsibility

AT Antiterrorism

ATC Antiterrorism Committee

ATCC Antiterrorism Coordinating Committee

ATEP Antiterrorism Enterprise Portal

ATF Bureau of Alcohol, Tobacco, and Firearms

ATO Antiterrorism Officer

ATOIC U.S. Army Terrorist Operations and Intelligence Center

ATWG Antiterrorism Working Group

BMM Borrowed Military Manpower

BTS Border and Transportation Security

CARVER Criticality, Accessibility, Recuperability, Vulnerability,
Effect and Recognizability

CBR Chemical, Biological, and Radiological

CBRNE Chemical, Biological, Radiological, Nuclear, or high yield Explosives

CbT Combating Terrorism

Cbt-RIF Combating Terrorism Readiness Initiative Fund

CCTV Closed Circuit Television

CI Counter Intelligence

CIA Central Intelligence Agency

COM Chief of Mission

CONUS Continental United States

COOP Continuity of Operations Plan

CoS Chief of Staff

COTS Commercial-off-the-shelf

CT Counter Terrorism

CVAMP Core Vulnerability Assessment Management Program

CWG Commercial-off-the-shelf Working Group

DASD (SO&CT) Deputy Assistant Secretary of Defense (Special Operations and Combating Terrorism)

DCIO Defense Criminal Investigative Organizations

DCIS Defense Criminal Investigative Service

DD AT/HD Joint Staff Deputy Director, Antiterrorism and Homeland Defense

DEA Drug Enforcement Agency

DHS Department of Homeland Security

DIA Defense Intelligence Agency

DIPNOTE Diplomatic Note

DIWS Defense Indications and Warning System

DOE Department of Energy

DOJ Department of Justice

DOS Department of State

DOT Department of Transportation

DTRA Defense Threat Reduction Agency

ECPs Entry Control Points

EEI Essential Elements of Information

EOC Emergency Operations Center

ESFs Emergency Support Functions

FBI Federal Bureau of Investigation

FEMA Federal Emergency Management Agency

FP Force Protection

FPCON Force Protection Conditions

FPED Force Protection Equipment Demonstration

FPTAS Flight Path Threat Analysis Simulation

FPWG Force Protection Working Group

GAO Government Accounting Office

GOTS Government-off-the-shelf

GSA General Services Administration

HAVs Heavy non-tactical Armored Vehicles

HAZMAT Hazardous Materials

HRB High Risk Billet

HRP High Risk Persons

HUMINT Human Intelligence

HVAC Heating, Ventilation, and Air-Conditioning

HSC Homeland Security Council

IDS Intrusion Detection Sensors

IED Improvised Explosive Device

IICT Interagency Intelligence Committee on Terrorism

IPL Integrated Priority List

IPT Installation Antiterrorism Program and Planning Tool

I&W Indications and Warning

IRT Incident Response Team

IVAs Integrated Vulnerability Assessments

JITF-CT Joint Intelligence Task Force- Combating Terrorism

JNLWD Joint Non-Lethal Weapons Directorate

JSIVA Joint Staff Integrated Vulnerability Assessment

JTTF Joint Terrorism Task Force

LAV Light non-tactical Armored Vehicles

LECIC Law Enforcement and Counterintelligence Community

LFA Lead Federal Agency

LIC Low Intensity Conflict

LVAs Local Vulnerability Assessments

MANPAD Man Portable Air Defense

MCIA Marine Corps Intelligence Agency

MDITDS Migration Defense Intelligence Threat Database System

MEVA Mission Essential Vulnerable Area

MI Military Intelligence

MSHARP Mission, Symbolism, History, Accessibility, Recognizability, Population, and Proximity

MTAC Navy Multiple Threat Alert Center

NCIS Naval Criminal Investigative Service

NSA National Security Agency

NSC National Security Council

NTAV Non-tactical Armored Vehicle

O/C Observer/Controllers

OOD Officer of the Deck

O&M Operations and Maintenance

PA Public Affairs

PAO Public Affairs Officer/Office

PBD Program Budget Decision

PCC Policy Coordinating Committee

PDM Program Decision Memorandum

POVs Privately Owned Vehicles

PPBE Planning, Programming, Budgeting and Execution System

PS Physical Security

PSD Protective Security Detail

PSEAG Physical Security Equipment Action Group

PSO Protective Service Operations

RA Risk Assessment

RAM Random Antiterrorism Measures

RDA Research, Development, and Acquisition

RIF Readiness Initiative Fund

ROE Rules of Engagement

RSO Regional Security Officer

S&T Science and Technology

SAF Small Arms Fire

SDF Self Defense Force

SECDEF Secretary of Defense

SECSTATE Secretary of State

SES Senior Executive Service

SIGINT Signal Intelligence

SJA Staff Judge Advocate

SOFA Status of Forces Agreement

SO/LIC Special Operations and Low Intensity Conflict

SOPA Senior Officer Present Afloat

SOPs Standard Operating Procedures

SOW Statement of Work

SSDF Shipboard Self-Defense Force

SWAT Special Weapons and Tactics

TA Threat Assessment

TACON Tactical Control

TICs Toxic Industrial Chemicals

TIMs Toxic Industrial Materials

TSA Transportation Security Administration

TRB Tactical Response Boat

TSWG Technical Support Working Group

TTPs Tactics, Techniques, and Procedures

TWG Threat Working Group

UFR Unfunded Requirement

USACIDC U.S. Army Criminal Investigation Command

USCG United States Coast Guard

USTRANSCOM United States Transportation Command

VA Vulnerability Assessment

WMD Weapons of Mass Destruction

WMDRF Weapons of Mass Destruction Response Functions